HUMBOLDT-UNIVERSITÄT ZU BERLIN

Angezapft

Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung

Diplomarbeit

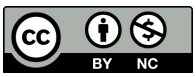
zum Erwerb des akademischen Grades Diplom-Informatiker

Angefertigt und vorgelegt von
Rainer Rehak

Gutachter:
Prof. Dr. Wolfgang Coy
Prof. Dr. Jens-Peter Redlich

Informatik in Bildung und Gesellschaft
Institut für Informatik
Mathematisch-Naturwissenschaftliche Fakultät II
Humboldt-Universität zu Berlin

Berlin, den 24. Juli 2015, korrigierte Version (v1.6)
Original vom 24. November 2011



Berlin, den 23. Juli 2012, Rainer Rehak (rehak@informatik.hu-berlin.de)

Kurzzusammenfassung

Diese Arbeit hat die *heimliche Online-Durchsuchung* zum Thema, eine verdeckte staatliche Maßnahme zur Informationsgewinnung mittels Infiltration informationstechnischer Systeme. Sie wurde und wird aktuell von deutschen Behörden verwendet, wobei ihr Einsatz nach wie vor hoch umstritten ist. Die Arbeit umreißt zunächst die technischen, rechtlichen und gesellschaftlichen Rahmenbedingungen und fasst die Diskussion der letzten Jahre zusammen, um danach die technisch-gesellschaftlichen Implikationen dieser Maßnahme zu analysieren.
Methodisch werden aus Aussagen von Akteuren der Politik, den gesellschaftlich-rechtlichen Rahmenbedingungen und den Prinzipien der modernen Rechnerarchitektur die konzeptionellen Anforderungen, Funktionen und Eigenschaften der Software einer solchen Maßnahme entwickelt. Aus dieser konzeptionellen Beschreibung können konkrete technische Eigenschaften abgeleitet werden, weil die beschriebenen Konzepte in einer gegebenen Computersystemarchitektur nicht beliebig implementierbar sind. An der so konstruierten prototypischen Software können dann notwendige technisch-gesellschaftliche Folgen, Fähigkeiten und Auswirkungen analysiert werden.
Diese hergeleiteten Eigenschaften werden dann mit dem Verfassungsgerichtsurteil zur Online-Durchsuchung aus dem Jahre 2008 und den dort geforderten technisch-rechtlichen Beschränkungen zusammengeführt. So können vom Gericht formulierte Anforderungen in reale Konsequenzen transformiert werden. Die gefundenen Ergebnisse sind wie folgt zusammenzufassen:

1. Eine Funktionsbeschränkung der Software kann weder sichergestellt noch belegt werden, daher muss immer die maximale Eingriffshürde zur Anwendung kommen.

2. Erlangte Daten haben grundsätzlich keinen Beweiswert, sofern sie keinen eigenen intrinsischen Personenbezug aufweisen (z. B. Bilder, die Personen zeigen).

3. Die Trennung von Telekommunikations- und Nichttelekommunikationsdaten ist technisch nicht hinreichend lösbar, daher muss immer — auch für eine Quellen-TKÜ — die maximale Eingriffshürde zur Anwendung kommen.

4. Der Kernbereich privater Lebensgestaltung ist praktisch immer betroffen, technischer Kernbereichsschutz ist prinzipiell nicht möglich.

Diese Resultate widersprechen der aktuellen politischen Praxis und implizieren, dass Exekutive und Legislative ihr Verständnis der Online-Durchsuchung konsequent korrigieren müssen. Die Arbeit soll darüber hinaus die aktuelle Diskussion generell um notwendige technische Grundlagen bereichern.

Inhaltsverzeichnis

Selbständigkeitserklärung

Ich erkläre, dass ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Berlin, den 24. November 2012

- - - - - - - - - - - - -
Rainer Rehak

Vorwort

Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt. Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, die Freiheit der Person ist unverletzlich (aus Art. 1 und 2 GG). Diese Werte sind die Grundwerte des deutschen Staatsverständnisses, vielleicht des modernen Rechtsstaatsverständnisses überhaupt[1] und begründen so die Hauptaufgabe des Staates in seiner Form als Institution. Diese Aufgabe besteht im Schutz der Würde und Freiheit des Einzelnen vor Eingriffen Dritter oder dem Staat selbst.
Dadurch wird offenbar, dass die grundsätzliche Debatte über das Spannungsfeld zwischen Sicherheit und Freiheit eine irreführende Themenbezeichnung hat. Sie impliziert eine Gleichwertigkeit der Begriffe *Sicherheit* und *Freiheit*, in Folge derer staatliches Handeln innerhalb dieser Ziele organisiert und abgewogen werden muss. Aus den Grundwerten des Staates ist diese Wertigkeit einer abstrakten Sicherheit jedoch nicht abzuleiten. Zu diskutierende Konfliktfälle handeln tatsächlich von widerstreitenden Freiheitsrechten verschiedener Personen. Es müssen daher unterschiedliche Freiheitsrechte gegeneinander abgewogen werden und das ist der eigentliche Diskurs.[2] Sicherheit ist folglich immer nur die Sicherheit der Freiheit; die beiden Begriffe sind mitnichten gleichwertig.

In der Konsequenz stellt sich auch die Frage nach den Bedingungen für die Freiheit des Menschen in einem digitalen Zeitalter. Eine Welt, in der vormals verborgene innere Vorgänge einer Person zunehmend nach außen verlagert werden und somit auch zunehmend zugreifbarer werden. Hier offenbart sich eine tatsächliche konkrete Aufgabe für den Sicherheitsbegriff als Gehilfen der Freiheit: Welche (neutralen) Infrastrukturen sind sinnvoll und welche sogar notwendig, wie können diese abgesichert werden, sind generell neue Regeln nötig und welche Effekte haben die „alten“ Regeln in der „neuen“ Welt?
Ein Novum dieser Art von Überlegungen und Fragen ist die große Abhängigkeit potenzieller Antworten von den Eigenheiten informationstechnischer Umsetzungsmöglichkeiten. Die Fähigkeiten und vor allem Grenzen der Technik müssen daher möglichst von Anfang an mitgedacht werden, denn eine Freiheitsbeschränkung wegen Nichtbeherrschbarkeit eingesetzter Technik wäre nicht mit den Grundwerten vereinbar.

[1] Siehe dazu Mill, *Über die Freiheit*, 1986.
[2] Detailliert behandelt in Bielefeldt, *Freiheit und Sicherheit im demokratischen Rechtsstaat*, Dezember 2004.

1 Einleitung

„*Yes this* and *no that* — that's what I call human nature."
Zhuang Zi

1.1 Auftakt

Erst kürzlich hat die Enquêtekommision „Internet und digitale Gesellschaft"[3] des Deutschen Bundestages ihren Zwischenbericht veröffentlicht.[4] Dies ist insofern ein Meilenstein für die Politik, als dass der nordrhein-westfälische Landtag noch vor vier Jahren in seiner Stellungnahme zur „Online-Durchsuchung" folgendes schrieb:

> Der Kernbereich privater Lebensgestaltung sei nicht (von der Online-Durchsuchung) betroffen, da der Bürger zur höchstpersönlichen Kommunikation nicht auf einen Personalcomputer angewiesen sei.[5]

Auch aktuell ist dieser Blick auf die private Computernutzung noch weit verbreitet, so befand im April 2010 das Landessozialgericht Nordrhein-Westfalen, „dass ein PC [...] nicht für ein an den herrschenden Lebensgewohnheiten orientiertes Leben benötigt werde".[6]

Diese Aussagen illustrieren auf sehr nüchterne Weise, welche Kluft zwischen angenommener und tatsächlicher Lebenswirklichkeit der Bevölkerung in Bezug auf Computernutzung bestand und vielleicht auch noch besteht. Schon im Jahre 2007 nutzten 70 Prozent der Bundesbürger einen Computer, und das nicht nur für geschäftliche E-Mailkommunikation[7] und arbeitsbezogene Informationsbeschaffung, sondern auch ganz privat für höchstpersönliche Interaktion,[8] soziale Netzwerke,[9] private Interessenausübung, Unterhaltung, Online-Einkauf sowie politische Partizipation.[10] Leider bezieht sich das politische Unwissen nicht nur auf die Rolle des Computers innerhalb des gesellschaftlichen Gefüges, sondern auch auf die technischen Grundlagen und generellen Funktionsweisen dieser Technologie.

Wahrscheinlich lag es an diesem Unverständnis der herrschenden Lebensgewohnheiten, dass

[3] `http://www.bundestag.de/internetenquete`.
[4] Enquêtekommision „Internet und digitale Gesellschaft", *Zweiter Zwischenbericht*, 21.10.2011.
[5] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 144.
[6] Landessozialgericht NRW Az: L 6 AS 297/10 B.
[7] Z. B. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. *39 Prozent der Personalchefs verlangen Bewerbung per Internet*, 2.5.2011.
[8] Kurz, *Kernbereichsschutz*, März 2009, Seite 2.
[9] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. *Halb Deutschland ist Mitglied in sozialen Netzwerken*, 13.4.2011.
[10] Siehe Hessischer Rundfunk & ZDF, *ARD/ZDF-Onlinestudie 2011*, 2011.

Ende 2006 in Nordrhein-Westfalen eine Ermächtigung zum heimlichen Aufklären des Internets verabschiedet wurde,[11] die das Bundesverfassungsgericht bald darauf wieder für nichtig erklärte und woraufhin es sogar ein neues Grundrecht formulierte, um solcher Art Ermächtigungen zukünftig sehr hohe Schranken aufzuerlegen. Besonders interessant an der Ableitung dieses neuen *Grundrechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme* aus dem allgemeine Persönlichkeitsrecht ist die Begründung:

> Soweit kein hinreichender Schutz vor Persönlichkeitsgefährdungen besteht, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist, trägt das allgemeine Persönlichkeitsrecht dem Schutzbedarf in seiner lückenfüllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet.[12]

Das Gericht erkennt die besondere gesellschaftliche Stellung an, die informationstechnischen Systemen heutzutage anheimfällt, und zeigt in dem Urteil, dass bei politischen Entscheidungen über Aspekte einer technisch durchsetzten Welt technischer Sachverstand und Kenntnis der gesellschaftlichen Verortung absolut notwendig sind. Es ist nicht die Aufgabe des Bundesverfassungsgerichtes, informationsgesellschaftlich-technische Wissensdefizite der Politik auszugleichen, daher müssen in derartig komplexen Entscheidungen entsprechende Spezialisten einbezogen werden, die die Ausgangssachverhalte analysieren und gesellschaftliche Konsequenzen technischer Entscheidungen so gut wie möglich abschätzen können, um sie dann verständlich darzustellen und zu erklären.
Wenn Menschen in einer Gesellschaft leben wollen, die sich in großem Maße auf Computertechnologie verlässt und ihr einen zentralen Stellenwert im gesellschaftlichen Miteinander einräumt, müssen die politisch gesetzten Rahmenbedingungen und Regeln dieser Tatsache auch Rechnung tragen. Die Einsetzung der oben genannten Enquêtekommission zeigt, dass auf diesem Feld Wissenslücken und Handlungsbedarf erkannt wurde. Die Notwendigkeit und Wirkung solcher Untersuchungen können dabei nicht zu hoch eingeschätzt werden, denn es geht um die Gestaltung der digitalen Welt von heute und morgen. Gesetze werden selten zurückgenommen und entstandener Schaden ist schwer zu beheben. Hinzu kommt die starke Stellung Deutschlands in Europa, so dass davon ausgegangen werden kann, dass die Gestaltung der hiesigen digitalen Landschaft auch über die Landesgrenzen hinaus Folgen haben wird, sei es als Teil einer Argumentation oder sogar als Leitkonzept.

In diesem Motivations- und Themenfeld ist auch diese Arbeit angesiedelt. Sie soll helfen, die gesellschaftliche Diskussion über Möglichkeiten und Notwendigkeit einer heimliche Online-Durchsuchung informatisch-sachlich zu unterstützen, indem die prinzipielle informationstechnische Struktur einer solchen Methode analysiert und technisch bedingte Effekte sowie Nebeneffekte aufgezeigt werden. Diese sollen dann in den gesellschaftlichen Kontext gesetzt und am

[11] § 5 Abs. 2 Nr. 11 in Verbindung mit § 7 Abs. 1, § 5 Abs. 3, § 5a Abs. 1 und § 13 VSG NRW in der Fassung des Gesetzes zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006 (GVBl NW 2006, S. 620).

[12] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 201.

Ende mit dem diesbezüglichen Urteil des Bundesverfassungsgerichts in Beziehung gebracht werden. Das in dieser Arbeit behandelte Problem besteht daher in der Frage, ob der technische Aspekt der heimlichen Online-Durchsuchung politisch-rechtlich ausreichend durchdrungen wurde. Oder anders ausgedrückt: Spiegeln sich die technischen Grenzen und Implikationen der Maßnahme in den rechtlich vorgegebenen Einsatzvoraussetzungen wider?

1.2 Einordnung des Problems

Im Dezember 2006 erhielt der nordrhein-westfälische Verfassungsschutz mit der *Ermächtigung zur Aufklärung des Internets* die Rechtsgrundlage für den Einsatz spezieller technischer Mittel zur heimlichen Infiltration und Durchsuchung informationstechnischer Systeme. Der Wortlaut des Kernaspekts:

> Die Verfassungsschutzbehörde darf nach Maßgabe des § 7 zur Informationsbeschaffung als nachrichtendienstliche Mittel die folgenden Maßnahmen anwenden:
> [...]
> 11. heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel.[13]

Insbesondere der Teil über den heimlichen Zugriff auf informationstechnische Systeme eröffnete eine bundesweite Diskussion über zweifelhafte Gesetzesgrundlagen und die Unvereinbarkeit derartiger Maßnahmen mit dem Grundgesetz. Für derartige Methoden der staatlichen Datenbeschaffung etablierte sich der Terminus „Online-Durchsuchung“, wobei die dafür eingesetzte „Remote Forensic Software (RFS)“[14] in Anlehnung an das Trojanische Pferd „Bundestrojaner“ oder „Staatstrojaner“ genannt wird.[15] In dieser Diskussion, die hauptsächlich in den Jahren 2007 und 2008 stattfand, muss man zwischen strafverfolgender und gefahrenabwehrender Online-Durchsuchung unterscheiden sowie zwischen der Nutzung auf Bundes- oder Länderebene. Die Diskussion wird im Folgenden kurz zusammengefasst.

Bereits 2005 wurde die gefahrenabwehrende Online-Untersuchung dem Bundesamt für Verfassungsschutz per geheimer Dienstanweisung unter dem damaligen Bundesinnenminister Otto Schily ermöglicht[16] und auch durchgeführt[17], worüber das Parlamentarische Kontrollgremium im Juli 2005 in Kenntnis gesetzt wurde.
2006 trat die strafverfolgende Online-Durchsuchung bei den Bundesstraforganen auf den Plan, wurde jedoch nach mehrmonatigem Streit durch die Instanzen vom Bundesgerichtshof (BGH)

[13] § 5 Abs. 2 Nr. 11, VSG NRW, eingefügt/geändert durch das Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20.12.2006.
[14] Interner Name des Bundeskriminalamtes (BKA), siehe Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Vorbemerkung.
[15] Heinrich, *Chaos Computer Club knackt Bundestrojaner*, 9.10.2011.
[16] dpa (Deutsche Presse Agentur), *Geheimdienste spitzeln schon seit Jahren*, 25.4.2007 und Beyer und Walter, *Videobeitrag: Wanze im Wohnzimmer – Online-Spitzelei durch den Verfassungsschutz*, 10.5.2007.
[17] Stark, „Digitale Spionage“, 2009.

am Anfang des Jahres 2007 wegen fehlender Rechtsgrundlage für unzulässig erklärt, was bis heute Stand der Dinge ist.[18]

Unabhängig davon entwickelte 2006 der damalige Bundesinnenminister Wolfgang Schäuble das „Programm zur Stärkung der inneren Sicherheit“, in dem u. a. die Notwendigkeit geäußert wurde, „entfernte PC auf verfahrensrelevante Inhalte durchsuchen zu können“, ohne vor Ort am Gerät zu sein. Hintergrund war die stetige Verlagerung der Kommunikation und Informationsaufbewahrung von organisierter Kriminalität, terroristischen Gruppen und Netzwerken hin zu digitalen Informationssystemen. Konkret ging es dabei um die Tatsache, dass weder verschlüsselte Daten auf Datenträgern bei Hausdurchsuchungen, noch verschlüsselte Kommunikation an Infrastrukturpunkten im Internet lesbar abgefangen werden können, was die Staatsorgane nach Ansicht Schäubles mit ihren damaligen Ermittlungsinstrumenten ins Hintertreffen geraten ließ: „Für die Sicherheitsbehörden gibt es immer weniger Ermittlungsansätze in der realen Welt, also müssen sie in der virtuellen Welt ermitteln, wenn sie den Tätern das Handwerk legen wollen.“[19] Um dieser Inhalte dennoch habhaft zu werden, müsse auf die Daten „vor der Verschlüsselung oder nach der Entschlüsselung, also am Computer des Täters“,[20] zugegriffen werden. Darüber hinaus „werden Daten heute oft sogar ganz in die Weiten des World Wide Web ausgelagert. Sie sind dann auf dem häuslichen PC gar nicht mehr vorhanden.“[21] Um die Daten dennoch zu erreichen, ist es in speziellen Fällen nötig, direkt auf das Informationssystem zuzugreifen oder es zu kontrollieren, solange es in Betrieb ist.

Auf der anderen Seite wurde diese Maßnahme u. a. von Bürgerrechtlern, Politikern und Juristen scharf kritisiert, da sie einen gravierenden Eingriff in die Grundrechte des Betroffenen darstellt und technisch sehr schwer fehlerlos zu bewerkstelligen sei, also nicht dem Verhältnismäßigkeitsgrundsatz genügen würde.[22] Die Maßnahme, so die Kritiker, verkenne die gesellschaftlich-soziale Stellung informationstechnischer Systeme für den modernen Bürger und habe eine derartige Eingriffstiefe in die Privatsphäre des Betroffenen, dass kein Zweck dieses Mittel rechtfertigen kann.[23] Die Debatte kulminierte 2007 in einer Verfassungsbeschwerde gegen das Land Nordrhein-Westfalen, in der u. a. die eingangs genannte Ermächtigung zur Aufklärung des Internets angegriffen wurde.

Im Februar 2008 wurden die angegriffenen Präventivnormen des nordrhein-westfälischen Landesverfassungsschutzgesetzes vom Bundesverfassungsgericht wegen Unvereinbarkeit mit dem Grundgesetz für ungültig erklärt und das neue *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* geboren. Das Gericht untersagte zwar weder die strafverfolgende noch die gefahrenabwehrende Nutzung einer heimlichen Online-Durchsuchung grundsätzlich,[24] setzte aber die Schranken für diesbezügliche Ermächtigungen wegen der eklatanten Verletzung des neuen Grundrechtes sehr hoch.[25]

[18] Bundesgerichtshof, *Kein heimlicher Zugriff auf ein Computersystem zum Zwecke der Strafverfolgung*, 25.11.2006.
[19] Schulzki-Haddouti und Ziegler, *Bundesinnenminister warnt vor zunehmender Netzspionage*, 22.5.2007.
[20] Rath, *„Am Computer des Täters ansetzen“*, 26.3.2007.
[21] A.a.O.
[22] Strafrechtsausschuss der Bundesrechtsanwaltskammer, *Stellungnahme der Bundesrechtsanwaltskammer zur sogenannten Online-Durchsuchung durch das Bundeskriminalamt zwecks Abwehr von Gefahren des internationalen Terrorismus*, Oktober 2007, Seite 4.
[23] Grell, *Harsche Kritik an Online-Durchsuchungen*, 3.2.2007.
[24] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 207.
[25] A.a.O. Absatz 247.

Kurz darauf drängte das Bundesland Bayern darauf, die Online-Durchsuchung zur Verfolgung schwerer Straftaten bundesweit zuzulassen, scheiterte mit seinem Antrag aber im Juli 2008 am Bundesrat.[26] Auf bayerischer Landesebene wurden die strafverfolgenden Befugnisse im August 2008 für Polizei[27] und Landesamt für Verfassungsschutz geschaffen.

An dieser Stelle sei angemerkt, dass das Bundesinnenministerium Anfang 2007 seine Ansicht kundtat, die Online-Durchsuchung sei dem Verfassungsschutz laut §8 Abs. 2 BVerfSG [28] bereits erlaubt,[29] was nach Ansicht von Experten in Regierung und Opposition jedoch nicht hinreichend gesetzlich geregelt ist.[30] Medienberichten zufolge wurde die Online-Durchsuchung von den Geheimdiensten bislang mindestens 2500 Mal durchgeführt,[31] auch im Inland.[32]

Trotz des Urteils des Bundesverfassungsgerichts zur Online-Durchsuchung blieb jedoch ein rechtlich-technischer Sachverhalt praktisch ungeklärt:
Mit einer Online-Durchsuchung ist es möglich, sich zu jeglichen Daten eines Systems Zugriff zu verschaffen, also auch zu Kommunikationsdaten. Würde man nun mit einer Online-Durchsuchung ein System infiltrieren, um nur dieser Telekommunikationsdaten habhaft zu werden, ginge die so „bedingte Gefährdung (der Person) [...] weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist".[33] Könne allerdings durch „technische Vorkehrungen und rechtliche Vorgaben"[34] sichergestellt werden, dass „sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt",[35] wäre Art. 10 Abs. 1 GG der „alleinige grundrechtliche Maßstab"[36] dieser dann Quellentelekommunikationsüberwachung (Quellen-TKÜ) genannten Maßnahme.
Im Falle der sichergestellten Beschränkung auf Telekommunikationsdaten würde folglich eine Quellen-TKÜ nach §100a StPO[37] als geheime Telekommunikationsüberwachung zulässig sein.
Ob sich die Beschränkung jedoch sicherstellen lässt, ist (unter anderem) eine technische Frage, die das Gericht leider gänzlich außen vor ließ.
Wäre es technisch nicht möglich, die Beschränkung auf Telekommunikationsdaten sicherzustellen, wären Quellen-TKÜ und Online-Durchsuchung technisch gesehen identisch. Es läge daher effektiv auch bei einer Quellen-TKÜ die hohe Eingriffsintensität einer Online-Durchsu-

[26] Krempl und Ziegler, *Bundesrat will heimliche Online-Durchsuchungen auf Terrorabwehr beschränken*, 4.7.2008.
[27] Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz — PAG) in der Fassung der Bekanntmachung vom 14. September 1990 (GVBl S. 397, BayRS 2012-1-1-I), zuletzt geändert durch § 2 des Gesetzes vom 22. April 2010 (GVBl S. 190).
[28] Damit auch dem Bundesnachrichtendienst (BND) nach §3 BNDG und dem Militärischen Abschirmdienst (MAD) nach §4 MADG.
[29] Bundesregierung der 16. Wahlperiode, *Drucksache 16/4803*, 23.3.2007, Antwort zu Frage 18 und 19.
[30] Rötzer, *Innenministerium: Verfassungsschutz, MAD und BND können Online-Durchsuchungen durchführen*, 24.3.2007.
[31] Stark, „Digitale Spionage", 2009.
[32] Krempl, *Medienbericht: BND hat bereits Online-Razzien durchgeführt*, 5.1.2008.
[33] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 188.
[34] A.a.O. Absatz 190.
[35] A.a.O. Absatz 190.
[36] A.a.O. Absatz 190.
[37] Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 5 des Gesetzes vom 23. Juni 2011 (BGBl. I S. 1266) geändert worden ist.

chung vor und § 100a StPO könnte für eine solche Maßnahme nicht zur Anwendung kommen.[38] Zudem spezifizierte das Gericht nicht, was in informationstechnischen Systemen überhaupt als Telekommunikationsdatum verstanden werden kann.
Trotz der auch aus dieser Problematik hervorgehenden heftigen Diskussionen über die Verfassungsmäßigkeit[39] solcher Maßnahmen wurden die gefahrenabwehrende Online-Durchsuchung als § 20k und die gefahrenabwehrende Quellentelekommunikationsüberwachung als § 20l des BKA-Gesetzes im Januar 2009 auf Bundesebene rechtlich geregelt,[40] in Rheinland-Pfalz ist die Online-Durchsuchung seit Anfang 2011 als § 31c POG für die dortige Polizei erlaubt.[41]
Die aktuelle Rechtslage der Online-Durchsuchung kann zusammengefasst der Tabelle 1 (Online-Durchsuchungsermächtigungen in Deutschland (Anfang 2012, in grau: Interpretation der Regelung strittig)) entnommen werden. Umstritten ist jedoch, ob die Quellen-TKÜ ein von der Online-Durchsuchung unterscheidbares Instrument ist.[42] Sie ist bislang nur im BKAG explizit geregelt und wird ansonsten mit § 100a StPO begründet,[43] was verfassungsrechtlich stark kritisiert wird.[44]

	Bundesebene	**Länderebene**
Gefahrenabwehr	Bundeskriminalamt, Verfassungsschutz, Militärischer Abschirmdienst (MAD), Bundesnachrichtendienst (BND)	Bayerische Polizei, Bayerischer Verfassungsschutz, Rheinland-Pfälzische Polizei
Strafverfolgung	keine Gesetzesgrundlage (laut BGH-Urteil)	keine Gesetzesgrundlage

Tabelle 1: Online-Durchsuchungsermächtigungen in Deutschland (Anfang 2012, in grau: Interpretation der Regelung strittig)

Auf Anfrage der bayerischen Grünenfraktion räumte das Münchner Justizministerium ein, dass die Online-Durchsuchung dort zwischen 2009 und 2010 insgesamt viermal eingesetzt worden

[38] Buermeyer und Bäcker, „Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO“, 2009.

[39] Damals Geiger, *Stellungnahme zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt BT-Drucksache 16/9588*, August 2008, Seite 18 ff. und Schaar, *Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Gesetzentwurf der Fraktionen der CDU/CSU und der SPD: Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, BT-Drs. 16/9588*, 15.9.2008, Seite 4 ff. heute Braun, „0zapftis – (Un)Zulässigkeit von “Staatstrojanern”“, 2011.

[40] Bundeskriminalamtgesetz vom 7. Juli 1997 (BGBl. I S. 1650), das zuletzt durch Artikel 2 des Gesetzes vom 6. Juni 2009 (BGBl. I S. 1226) geändert worden ist.

[41] Rheinland-pfälzisches Polizei- und Ordnungsbehördengesetz (POG) vom 10. November 1993, das zuletzt mehrfach durch Artikel 1 des Gesetzes vom 15.2.2011 (GVBl. S.26) geändert worden ist.

[42] Vergleiche Bäcker, „Das IT-Grundrecht“, 2009, Seite 22 ff.

[43] Siehe z. B. Anfrage zum Plenum der Abgeordneten Susanna Tausendfreund anlässlich der Plenarwoche in der 23. KW 2011, Bayerischer Landtag.

[44] Buermeyer und Bäcker, „Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO“, 2009, Seite 9 und Braun, „0zapftis – (Un)Zulässigkeit von “Staatstrojanern”“, 2011, Seite 686.

war und aktuell immer noch wird,[45] auch in der Form einer Quellen-TKÜ. Deutschlandweit — alle Behörden zusammengenommen — wurde die Maßnahme, entgegen der ursprünglich erwarteten einstelligen Fallzahl pro Jahr,[46] bisher etwa 100 Mal durchgeführt.[47]
Die praktische Ausgestaltung der Quellen-TKÜ ist u. a. wegen des folgenden exemplarischen Falles interessant und hochbrisant:
Mitte 2009 wurde einem Pharmahändler aus Bayern, gegen den wegen Verstoßes gegen das Betäubungsmittelgesetz ermittelt wird, verdeckt bei einer Flughafenkontrolle eine Online-Durchsuchungssoftware auf den Laptop aufgespielt. Beantragt vom Landeskriminalamt Bayerns (LKA Bayern) und bewilligt vom Amtsgericht Landshut sollte diese Software „die Überwachung und Aufzeichnung des Telekommunikationsverkehrs“ des Beschuldigten übernehmen, da dieser nur die verschlüsselt funktionierende Internettelefoniesoftware Skype verwendete;[48] es handelte sich um eine oben beschriebene Quellen-TKÜ.
Das Amtsgericht Landshut hatte die Maßnahme im April 2009 basierend auf dem Paragraphen 100a der Strafprozessordnung (§ 100a StPO) beschlossen, laut welchem „ohne Wissen der Betroffenen [...] die Telekommunikation überwacht und aufgezeichnet werden“ darf. Dies umfasst nach aktueller Auslegung auch E-Mails, Chats und ähnliches, jedoch nur während des Kommunikationsvorganges. Die Richter untersagten daher explizit das Sammeln von darüber hinausgehenden Daten durch die Quellen-TKÜ.[49]
Dieser Beschluss basierte wieder auf der umstrittenen Annahme, dass eine Quellen-TKÜ eine normale Telekommunikationsüberwachung sei und keine Online-Durchsuchung. Diese wäre nach Artikel 34d des Bayerischen Polizeiaufgabengesetzes (PAG) nur gestattet, um eine dringende Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person abzuwehren, was im vorliegenden Fall (banden- und gewerbsmäßiger Handel und Ausfuhr von Betäubungsmitteln) nicht zutrifft. Eine Klärung der rechtlichen Vorgaben steht bis dato noch aus.
Hinzu kommt, dass die umstrittene Maßnahme zusätzlich zu Gesprächsinhalten bei aktivem Browser aller 30 Sekunden einen Screenshot übermittelte. Nach erfolgloser Beschwerde des Anwalts des Beschuldigten vor dem Amtsgericht befand in nächster Instanz das Landgericht Folgendes:

> Jedoch war der Vollzug des Beschlusses vom 02.04.2009 insoweit rechtswidrig, als im zeitlichen Abstand von 30 Sekunden Screenshots von der Bildschirmoberfläche gefertigt wurden, während der Internet-Browser aktiv geschaltet war. Denn nach Auffassung der Kammer besteht für das Kopieren und Speichern der grafischen Bildschirminhalte, also der Fertigung von Screenshots, keine Rechtsgrundlage, weil zum Zeitpunkt dieser Maßnahmen noch kein Telekommunikationsvorgang stattfindet. Es kann nicht außer Acht gelassen werden, dass — anders als bei der Internettelefonie — die E-Mail zum Zeitpunkt ihrer „Ablichtung“ mittels

[45] Bayerisches Staatsministerium der Justiz und für Verbraucherschutz, *Drucksache 16/8125*, 29.04.2011.
[46] Vergleiche Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 135.
[47] Patalong, *Behörden spähten 100-mal Computer aus.*
[48] Beschluss vom 2.4.2009 Az: II Gs 833/10 AG Landshut.
[49] Beschluss vom 2.4.2009 Az: II Gs 833/10 AG Landshut.

„Screenshot“ noch nicht unmittelbar vor ihrer Versendung steht, insbesondere auch wieder geändert oder gelöscht werden könnte.[50]

Genau betrachtet stellt sich der geringste Teil der Aktivitäten im Browser als Telekommunikationsvorgang dar, denn selbst bei ausschließlichem E-Mailschreiben und Chatten wäre jeweils nur das eigentliche Senden ein Telekommunikationsvorgang, nicht aber das Tippen selbst. Nimmt man nun eine durchschnittliche Browsernutzung (vom Zeitung lesen bis zum Anschauen von Videos) an, wird die Eingriffstiefe des Bildschirmfotoanfertigens sichtbar. In der Konsequenz erklärte das Landgericht Landshut die Maßnahme im Nachhinein für unzulässig.

Die Diskussion um Quellen-TKÜ und Online-Durchsuchung ebbte nach diesem Vorfall nur langsam ab, kam aber auch nicht voran. Dies war ein schlimmer Zustand für einen Rechtsstaat, denn die Überwachungsmaßnahme, die höchstrichterlich — es wurde keine Berufung eingelegt — für unzulässig erklärt worden war, wurde weiterhin eingesetzt; in vollem Bewusstsein der (wider-)rechtlichen Lage.[51]
Im Oktober 2011 kam wieder Bewegung in den Diskurs, denn der Chaos Computer Club war mehrerer Binärdaten von Quellen-TKÜ habhaft geworden. Er hatte diese analysiert und technisch den Beleg liefern können, dass die Software für Quellen-TKÜ und Online-Durchsuchung im vorgefundenen praktischen Einsatz ein und dieselbe Software, also ineinander transformierbar ist.[52]

Diese aktuellen Geschehnisse um die Veröffentlichung des Staatstrojaners, die umstrittene Gesetzeslage bei Online-Durchsuchung und Quellen-TKÜ, deren bewusst rechtswidriger Einsatz sowie deren kritisierte Nutzung durch die Geheimdienste[53] zeigen, dass der Diskurs über die Online-Durchsuchung wieder in vollem Gange ist[54] und — mit Blick auf die Aktualität, Tragweite[55] und gesellschaftliche Bedeutung des Themas[56] — auch sein sollte.

2 Methodik und Begriffsklärung

2.1 Methodik der Arbeit

Zunächst werden anhand der Aussagen von verantwortlichen Politikern, Staatsorganen, anderen an der Diskussion beteiligten Personen und insgesamt des rechtlichen, technischen und gesellschaftlichen Kontextes der Situation konzeptionelle Anforderungen an eine heimlichen Online-Durchsuchung formuliert. Diese beschreiben bestimmte Eigenschaften, Funktionen und

[50] Beschluss vom 20.01.2011 Az: 4 Qs 346/10 LG Landshut.
[51] Trotz des Beschlusses der Rechtswidrigkeit der Bildschirmfoto-Quellen-TKÜ am 20.01.2011 (Az: 4 Qs 346/10 LG Landshut), wurden laufende Maßnahmen nicht abgebrochen. Bayerisches Staatsministerium der Justiz und für Verbraucherschutz, *Drucksache 16/8125*, 29.04.2011.
[52] Chaos Computer Club, *Chaos Computer Club analysiert Staatstrojaner*, 8.10.2011.
[53] Stark, „Digitale Spionage“, 2009.
[54] Umfrage zum Einsatz der Online-Durchsuchung: 43% der Bürger sind „dafür“, 52% „dagegen“ ZDF, *Politbarometer 14.10.201*, 14.10.2011.
[55] Krempl, *Britische Regierung drängt auf EU-weite heimliche Online-Durchsuchungen*, 5.1.2009.
[56] Wilkens, *Mehr als 50 Millionen Internetnutzer in Deutschland*, 4.7.2011.

„Verhaltensweisen“, die notwendig oder zumindest sehr wünschenswert für eine sinnvolle Anwendbarkeit der Online-Durchsuchung sind. Dies umfasst auch negative Anforderungen, also Folgen, Umstände und Aktivitäten des technischen Aspekts der Maßnahme, die auf jeden Fall vermieden werden müssen oder deren Auftreten zumindest sehr unwahrscheinlich sein muss.

Aus dieser konzeptionellen Beschreibung können konkrete technische Eigenschaften abgeleitet werden. Dies ist möglich, weil die beschriebenen Konzepte und Fähigkeiten in einer gegebenen Computersystemarchitektur nicht beliebig implementierbar sind. Oder anders ausgedrückt: Die aktuelle Computersystemarchitektur definiert funktionale Abhängigkeiten, in denen bestimmte Funktionen nur auf bestimmte Weise realisiert werden können.

Die so abgeleiteten technischen Eigenschaften werden einer Analyse unterzogen, wobei das Augenmerk auf unbeabsichtigte Eigenschaften, technische Grenzen und ungewollte Nebeneffekte gerichtet ist, was insofern keine Unausgewogenheit darstellt, als dass die beabsichtigten Funktionen und Eigenschaften einer heimlichen Online-Durchsuchung den Ausgangspunkt der Betrachtung bilden.

Das sich ergebende Bild der beabsichtigten und unbeabsichtigten Funktionen sowie Möglichkeiten einer heimlichen Online-Durchsuchung wird daraufhin in den generellen informationsgesellschaftlich-rechtlichen Kontext eingebettet, um deren über technische Aspekte hinausgehende Wechsel- und Auswirkungen aufzuzeigen. Dabei werden stets die technischen Ursachen der nichttechnischen Folgen erläutert.

Im Anschluss erfolgt eine Zusammenfassung des eingangs erwähnten Urteils des Bundesverfassungsgerichtes zu heimlichen Online-Durchsuchungen mit spezieller Analyse und Bewertung der Entscheidung aus technischer Sicht. Das Gericht hatte neben der Aufhebung der damaligen Regelung für den heimlichen Zugriff auf informationstechnische Systeme auch hohe Schranken für eine erneute Schaffung derartiger gesetzlicher Grundlagen formuliert, die den informationsgesellschaftlichen Folgen, Möglichkeiten und Risiken einer solchen Maßnahme Rechnung tragen sollen.

Mit dieser zweifachen Herangehensweise ist es möglich, das vorher entwickelte Bild der beabsichtigten und unbeabsichtigten Konsequenzen und Eigenschaften einer heimlichen Online-Durchsuchung mit der Kritik und den Anforderungen des Bundesverfassungsgerichtes in Deckung zu bringen. Dies macht es möglich, konkrete Aussagen für den Einsatz verfassungsmäßiger heimlicher Online-Durchsuchungen zu erarbeiten, die die technischen Möglichkeiten und Grenzen dieser Maßnahme mit einbeziehen. Technikabhängige Implikationen des Urteils können somit aufgelöst werden.

Resultat ist die Sichtbarmachung des vom Gericht vorgegebenen verfassungsmäßigen Rahmens für derartige rechtlich-technische Regelungen und die dadurch mögliche Kritik der aktuellen Rechts- und Anwendungspraxis.

Die eigentliche Arbeit beginnt mit dem Definitionsteil, der die in dieser Diskussion wichtigen Begriffe wie *informationstechnisches System* oder *Hausdurchsuchung* ordnen und erklären soll, soweit dies mit Blick auf das Thema sinnvoll ist.

2.2 Informationstechnisches System

Der Begriff *System* beschreibt ein Konzept, nach dem ein logisches Ganzes als aus miteinander interagierenden Komponenten bestehend betrachtet werden kann. Dabei können die Bestandteile selbst wiederum auch Systeme sein.[57] Die Reichweite eines Systemkonzeptes hängt davon ab, wie der Begriff „interagieren“ im konkreten Fall definiert wird. Im vorliegenden Kontext geht es um informationstechnische Interaktion, also technikgestützte Informationsverarbeitung oder konkreter: Datenverarbeitung. Ein informationstechnisches System bezeichnet daher die Menge aller Komponenten, die an einer bestimmten — auch zeitlich ausgedehnten — Datenverarbeitung beteiligt sind. Hier hängt der Begriffsradius vom Verständnis des Wortes „bestimmten“ ab,[58] doch das ergibt sich jeweils aus dem Kontext der Begriffsverwendung.

Allgemein sind in dieser Arbeit mit dem Begriff *informationstechnisches System* digitale Computer beliebiger Größe gemeint. Auf eine detailliertere Definition kann hier verzichtet werden, da sie keinen Erkenntnisgewinn für das vorliegende Thema bedeuten würde. Wichtig ist darüber hinaus, wie die Akteure des hier behandelten Diskurses den Begriff verstehen.
Das Bundesministerium des Innern versteht allgemein unter einem informationstechnischen System „ein System [...], welches aus Hard- und Software sowie aus Daten besteht, das der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten dient. [...] Im Sinne der obigen Definition eines „informationstechnischen Systems“ handelt es sich auch beim Internet um ein solches System“.[59]
Auch das Bundesverfassungsgericht versteht unter einem informationstechnischen System ein technisches System, das Informationen verarbeitet. Dabei ist es irrelevant, ob die Informationen nur aufgenommen, gespeichert, weitergeleitet, bearbeitet oder ausgegeben werden. Der Begriff „System“ verweist darauf, dass nicht nur Geräte wie Desktopcomputer, Laptops, Mobiltelefone, PDAs, Router oder Navigationsgeräte und deren jeweilige Peripherie bezeichnet werden sollen, sondern auch Netzwerke und andere Verbünde dieser Geräte oder Netzwerke.[60]
Das Bundesverfassungsgericht geht in seiner Definition noch einen Schritt weiter und definiert die Möglichkeit einer Personenzuweisung von informationstechnischen Systemen:
Auch nicht-lokal vorgehaltene Daten eines Nutzers werden als Teil seines informationstechnischen Systems verstanden, wenn er es „als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er (darüber) [...] selbstbestimmt verfügt“.[61] Beispiele sind die eigenen E-Mails auf Servern von E-Mailanbietern, auf die man nur über ein Webinterface zugreift, verteilte Ordner, mit denen Daten über mehrere eigene Rechner mithilfe des Internets abgeglichen werden können, oder persönliche Adressbücher und Kalender auf Webservern. Das informationstechnische System einer Person bezeichnet daher die Menge aller Komponenten, die von der Person zur Datenverarbeitung verwendet werden.
Es nimmt darüber hinaus eine Unterscheidung in zwei (nicht trennscharfe) Klassen vor, wobei nur die letztere für diese Arbeit von Belang sein wird:

[57] Schneier, *Secrets and Lies*, 2004, Seite 5 ff.
[58] Vergleiche dazu auch Anderson, *Security Engineering*, 2008, Seite 13.
[59] Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seiten 2 und 4.
[60] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 4.
[61] A.a.O. Absatz 206.

Einerseits die Klasse der informationstechnischen Systeme, die nach ihrer „technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich [...] (verarbeiten) — zum Beispiel nicht vernetzte elektronische Steuerungsanlagen der Haustechnik“,[62] und andererseits die, die „einen Einblick in wesentliche Teile der Lebensgestaltung einer Person [...] gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit [...] erhalten“[63] können.

Vertraulichkeit und Integrität informationstechnischer Systeme

In Bezug auf informationstechnische Systeme haben die Begriffe Vertraulichkeit und Integrität ihren Ursprung in der Datensicherheit, wo sie zwei wesentliche Schutzziele beschreiben. Vertraulichkeit bedeutet, dass ausschließlich befugte Personen lesenden Datenzugriff auf das System oder Teile davon haben.[64] Integrität dagegen bedeutet, dass ausschließlich befugte Personen schreibenden Datenzugriff auf das System oder Teile davon haben;[65] in der Folge bedeutet ein Verlust der Integrität eines Systems immer den Verlust der exklusiven Kontrolle darüber.[66] Für das informationstechnische System einer Person entscheidet nur sie selbst, wer befugt ist.
Das Bundesverfassungsgericht definiert die Begriffe sehr ähnlich und sieht insbesondere dann die Integrität verletzt, wenn „auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können.“[67]

2.3 Hausdurchsuchung

Bei einer Hausdurchsuchung werden Wohnräume oder anderweitig genutzte Räume des Betroffenen durchsucht. Zweck kann im Wesentlichen die Ergreifung eines Täters, die Auffindung von Beweismitteln (§ 102 StPO[68]) oder die Abwehr einer durch konkreten Anlass gegebenen Gefahr sein. Als staatliche Maßnahme mit Grundrechtseingriff gilt der Grundsatz der Verhältnismäßigkeit.[69]
Bei einer Hausdurchsuchung müssen neben den durchsuchenden Beamten auch der anordnende Richter bzw. Staatsanwalt zugegen sein oder — wenn möglich — ein Gemeindebeamter bzw. zwei Mitglieder der Gemeinde, die keine Polizisten sind (§ 105 StPO). Während der Durchsuchung hat der Betroffene das Recht, zugegen zu sein, oder es ist — wenn möglich — sein Vertreter oder ein erwachsener Angehöriger, Hausgenosse oder Nachbar hinzuzuziehen (§ 106 StPO).
Am Ende der Durchsuchung ist dem Betroffenen schriftlich mitzuteilen, was der Grund der Durchsuchung ist und ggf. welcher Straftat er verdächtigt wird. Darüber hinaus muss ihm eine Auflistung der aus den Räumen entfernten Gegenstände übergeben werden (§ 107 StPO).

[62] A.a.O. Absatz 202.
[63] A.a.O. Absatz 203.
[64] Vergleiche Anderson, *Security Engineering*, 2008, Seite 13 ff.
[65] Vergleiche a.a.O. Seite 14.
[66] Schneier, *Secrets and Lies*, 2004, Seite 45.
[67] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 204.
[68] Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 5 des Gesetzes vom 23. Juni 2011 (BGBl. I S. 1266) geändert worden ist.
[69] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Durchsuchung*, 5.5.2011, Absatz 16.

Zusammenfassend ist eine Hausdurchsuchung trotz ihres im Grundsatz auf Offenheit angelegten, körperlichen Charakters[70] ein schwerwiegender Grundrechtseingriff.[71]

2.4 Kernbereich privater Lebensgestaltung

Der Kernbereich privater Lebensgestaltung ist ein vom Bundesverfassungsgericht geprägter Begriff, der den innersten, persönlichsten Bereich einer Person beschreibt und ihn somit juristisch handhabbar macht. Das Gericht leitet dessen Anerkennung aus der Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG ab, wobei der Kernbereich absoluten Schutz genießt,[72] d. h., er ist der öffentlichen Gewalt schlechthin entzogen. Selbst schwerwiegende Interessen der Allgemeinheit können Eingriffe in diesen Bereich nicht rechtfertigen, weswegen eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes nicht stattfinden kann.[73]
Den Inhalt des Kernbereichs definiert das Gericht so:

> Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen. Vom Schutz umfasst sind auch Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität. Die Möglichkeit entsprechender Entfaltung setzt voraus, dass der Einzelne über einen dafür geeigneten Freiraum verfügt.[74]

Die jedem Menschen unantastbar gewährte Freiheit zur Entfaltung in den ihn betreffenden höchstpersönlichen Angelegenheiten würde verletzt werden, wenn der Staat in den Kernbereich eingreifen könnte.[75] Im Urteil zum „Großen Lauschangriff“ unterstrich das Gericht, dass „der Schutz des Kernbereichs der Privatsphäre erfordere, dass die Rechtsordnung schon hinsichtlich der Zulässigkeit des Abhörens sachgerecht unterscheide und nicht erst bei der Frage der Verwendung der gewonnenen Erkenntnisse“.[76]

Zur positiven Bestimmung des Kernbereichs verweist das Gericht darauf, dass er ausschließlich aus sich heraus, vom Personhaften her, bestimmt werden muss.[77] Zur negativen Bestimmung zieht das Gericht heran, in welcher Art und Intensität ein Sachverhalt aus sich heraus die Belange der Gemeinschaft oder die Sphäre anderer berührt.[78] Darüber hinaus dürfen externe

[70] Bundesgerichtshof, *Kein heimlicher Zugriff auf ein Computersystem zum Zwecke der Strafverfolgung*, 25.11.2006, Abschnitt 4.
[71] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Durchsuchung*, 5.5.2011, Abschnitt 14.
[72] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum großen Lauschangriff*, 3.3.2004, Leitsatz 2.
[73] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum Tagebuchinhalt I*, 14.9.1989, Absatz 25.
[74] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum großen Lauschangriff*, 3.3.2004, Absatz 120.
[75] A.a.O. Absatz 118.
[76] A.a.O. Absatz 61.
[77] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum Tagebuchinhalt I*, 14.9.1989, Absatz 48.
[78] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum Beischlaf zwischen Geschwistern*, 26.2.2008, Absatz 33.

Erfordernisse nicht auf die Bestimmung des Kernbereichs einwirken, sonst läge eine Instrumentalisierung der Menschenwürde vor.[79]

Die praktische Anwendung des Kernbereichskonzeptes ist jedoch sehr schwierig, da fragliche Sachverhalte nur gemäß ihrem Inhalt klassifiziert werden, nicht aber ihrer räumlichen Positionierung oder anderen kontextuellen Kriterien nach. Dies hat zwar einerseits zur Folge, dass auch Telekommunikationssachverhalte unter den Kernbereichsschutz fallen können,[80] andererseits müssen intime Aufzeichnungen wie Tagebucheinträge oder sensible Notizen nicht unbedingt Teil des Kernbereichs sein, wenn sie Aufschluss über strafbare Handlungen geben.[81]
In jüngster Zeit wurde der absolute Schutz des Kernbereichs privater Lebensgestaltung vom Bundesverfassungsgericht ein Stück weit verändert, denn um ihn nun sicherzustellen, genüge es, die von einer Online-Durchsuchung gefundenen und übermittelten Dateien auf Behördenseite einer Durchsicht zu unterziehen, bevor sie verwertet würden.[82]

2.5 Heimliche Online-Durchsuchung

Die Bezeichnung „heimliche Online-Durchsuchung“ ist ein rechtlich unscharfer Oberbegriff[83] für den verdeckt — also ohne Kenntnis der Betroffenen[84] — durchgeführten Zugriff auf informationstechnische Systeme durch Staatsorgane als Mittel der Datenbeschaffung. Der Begriff ist insofern irreführend, als dass unter einer *Durchsuchung* eine „im Grundsatz auf Offenheit angelegte Maßnahme“[85] vor Ort verstanden wird. Trotzdem Online-Überwachung weitaus treffender wäre, hat sich der Terminus *Online-Durchsuchung* durchgesetzt.
Unter dem Gesichtspunkt der Datensicherheit ist die Online-Durchsuchung eine Infiltration eines Systems,[86] denn sie verletzt die Vertraulichkeit und Integrität des Systems. Unter Integrität wird hier nicht nur die Konsistenz der Daten und des Systems verstanden, sondern auch — wie oben erwähnt, dass nur befugte Personen Datenzugriff bzw. Kontrolle über das System ausüben können.
Weil die hohe Komplexität moderner vernetzter Computer diesen Kontrollaspekt objektiv aufweicht,[87] kann und muss die Erwartungshaltung des Benutzers gegenüber seinem System als „sein System“ in das Integritätsverständnis einbezogen werden. Aus Sicht der Datensicherheit existiert neben Vertraulichkeit und Integrität ein weiteres Schutzziel, die Verfügbarkeit. Sie beschreibt die Zugreifbarkeit von Daten bzw. die allgemeine Benutzbarkeit des Systems.[88]

[79] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum Tagebuchinhalt I*, 14.9.1989, Absatz 48.
[80] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum großen Lauschangriff*, 3.3.2004, Absatz 136.
[81] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum Tagebuchinhalt II*, 1.2.2006, Absatz 7.
[82] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 132.
[83] Siehe Buermeyer, „Die Online-Durchsuchung. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme.“, 2007, Seite 154.
[84] In dieser Arbeit: Jeder, der vom hoheitlichen Zugriff auf ein von ihm benutztes, informationstechnisches System berührt ist.
[85] Bundesgerichtshof, *Kein heimlicher Zugriff auf ein Computersystem zum Zwecke der Strafverfolgung*, 25.11.2006, Absatz 4.
[86] Hansen und Pfitzmann, „Techniken der Online-Durchsuchung“, 2008, Seite 132, siehe auch Silberschatz, Galvin und Gagneand, *Operating System Concepts*, 2009, Seite 591 ff.
[87] Z. B. Webmailing in Internetcafés, Schneier, *Secrets and Lies*, 2004, Seite 6 ff.
[88] A.a.O. Seite 122.

Die Verfügbarkeit des Systems sollte weiter gewährleistet sein, damit dem Betroffenen vorgetäuscht werden kann, ein intaktes, von ihm kontrolliertes System vorzufinden. Warum die genannten Verletzungen notwendigerweise stattfinden, wird in Abschnitt 3 (Die Online-Durchsuchung en detail) erklärt.

Zweck der Maßnahme ist, wie in Unterabschnitt 1.2 (Einordnung des Problems) ausgeführt, die verdeckte Informationsbeschaffung, also unbemerktes Suchen und Speichern von Daten des Systems. Unterscheiden kann man derartige Maßnahmen anhand der Art der gesammelten Informationen und der Mittel, mit denen sie gesammelt werden. Eine erschöpfende Auflistung der Möglichkeiten ist im Rahmen dieser Arbeit nicht sinnvoll, daher werden hier nur beispielhaft einige erwähnt.

2.5.1 Hardwarebasierte Online-Durchsuchung

Zum einen können in das zu infiltrierende System verdeckt Hardwarekomponenten eingebracht oder vorhandene verändert werden. Möglich ist der Einbau von Hardwarekeyloggern, die die Tastenanschläge an einem Computer registrieren und speichern. Sie können direkt in die Tastatur eines Computers, in die Verbindung zwischen Tastatur und Computer oder auch in den Computer selbst eingebaut werden. Beim späteren Auslesen der gesammelten Daten können Usernamen, Passwörter und andere textbasierte Zugangsinformationen extrahiert werden, um sich im Anschluss Zugriff auf verschlüsselte Datenträger, Onlineprofile oder andere Zugänge zu verschaffen. Diese Maßnahme verletzt hauptsächlich die Vertraulichkeit eines informationstechnischen Systems.
Weiter ist die Einbringung von zusätzlichen geheimen Speichermedien denkbar, wodurch Speicherplatz auf dem System geschaffen würde, der von anderen Komponenten der Online-Durchsuchung genutzt werden könnte, aber mit hoher Wahrscheinlichkeit vom Betroffenen unbemerkt bliebe. Auch andere Hardwaremodifikationen — z. B. der Einbau von Funkmodulen, GPS-Empfängern usw. — sind denkbar, werden aber derzeit nicht öffentlich diskutiert.

Analyse von Abstrahlungen / TEMPEST

Elektrische und elektronische Bauteile in technischen Geräten erzeugen in aktivem Zustand elektromagnetische (engl. abgekürzt „TEMPEST“ genannt) und akustische Abstrahlungen. Dies ist teilweise gewollt (Leuchten des Bildschirms), aber größtenteils für die normale Operation des Gerätes unbedeutend (Tastaturgeräusch, Ultraschall von Piezoelementen).
Mit feinen Sensoren (z. B. Antennen oder Mikrofonen) ist es möglich, diese Abstrahlungen auch aus einiger Entfernung noch aufzufangen und zu analysieren. Gerade so komplexe elektronische Systeme wie Computer besitzen eine Vielzahl dieser Komponenten[89] und sind Gegenstand dementsprechender Forschung.
Bei einem Angriff wird anhand dieser Abstrahlungen eines informationstechnisches Systems versucht, die gerade verarbeiteten Daten zu rekonstruieren. Es ist bereits gelungen, aus den

[89] Pfitzmann, *Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft*, 26.9.2007, Seite 3 und 6.

Geräuschen einer Tastatur die getippten Buchstaben und aus den elektromagnetischen Feldern der Grafikkarte Teile des Bildschirminhalts zu berechnen.[90]

Die genauesten Ergebnisse erhält man durch die Analyse der Computermonitorabstrahlung, wenn es sich um einen Röhrenmonitor handelt. So ist es teilweise sogar möglich, den aktuellen Bildschirminhalt genau zu ermitteln.[91]

Nur bei der Analyse von Abstrahlungen wird die Integrität des informationstechnischen Systems nicht kompromittiert. Diese Art der Überwachung funktioniert auch dann in Echtzeit, wenn das informationstechnische System nicht/nie mit dem Internet verbunden wird.

2.5.2 Softwarebasierte Online-Durchsuchung

Bei der softwarebasierten Realisierung einer heimlichen Online-Durchsuchung wird das informationstechnische System der Zielperson mittels einer verdeckt in das System eingebrachten Software einmalig durchsucht (Online-Durchsicht) oder dauerhaft durchsucht und überwacht (Online-Überwachung).[92] Daten, die vorher definierten Suchkriterien entsprechen, werden im Anschluss der zuständigen Stelle zugeführt.[93]

Durch eine Dauerüberwachung werden auch flüchtige Datenströme, verschlüsselte Daten und Veränderungen an Daten zum Gegenstand der Maßnahme. So sind auch z. B. softwarebasierte Keylogger, die verdeckte Speicherung gelöschter Dateien oder der Mitschnitt laufender Computeraktivitäten wie etwa Online-Banking denkbar. Daten der Fernkommunikation sind nicht Ziel der Maßnahme.[94]

Die Online-Durchsuchungs-Software (ODS)

In dieser Arbeit werden die Begriffe *Online-Durchsuchung*, *Online-Durchsuchungs-Software (ODS)* und *Remote-Forensic-Software (RFS)* klar unterschieden. Mit Online-Durchsuchung ist die Maßnahme im rechtlichen Sinne gemeint; die ODS ist ein konzeptionell-prototypisches Modell einer Software, mit der Online-Durchsuchungen durchgeführt werden können, und RFS oder RFS-Implementation ist eine konkrete implementierte Software, mit der Online-Durchsuchungen durchgeführt wurden oder werden sollen. In die letzte Kategorie fällt z. B. der sogenannte Bayerntrojaner.[95]

Es werden wenige Verweise auf RFS-Implementationen erfolgen, da sich diese Arbeit zur Aufgabe gemacht hat, prinzipielle Eigenschaften, Funktionen und Folgen einer Online-Durchsuchung und der dafür nötigen Online-Durchsuchungs-Software zu analysieren. Die grundsätzlichen Probleme sind von der konkreten Implementation unabhängig und werden daher anhand der ODS behandelt, um den Rahmen des technisch Machbaren abzustecken.

[90] Bogk (Chaos Computer Club), *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007, Seite 9.

[91] Eck, „Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?“, 1985.

[92] Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Vorbemerkung.

[93] A.a.O. Vorbemerkung.

[94] A.a.O. Seite 7.

[95] Siehe Chaos Computer Club, *Report 23*, 8.10.2011.

2.6 Quellen-Telekommunikationsüberwachung (Quellen-TKÜ)

Die Quellentelekommunikationsüberwachung (Quellen-TKÜ) ist eine staatliche Maßnahme mit dem Zweck, Telekommunikationsdaten an einem informationstechnischen System abzufangen. Sie ist angedacht, wenn die Kommunikationsdaten verschlüsselt übertragen werden, also nicht sinnvoll an der Telekommunikationsinfrastruktur abgefangen werden können.[96]

Quellentelekommunikationsüberwachungs-Software (QTKÜS)

Die Quellen-TKÜ wird nur softwarebasiert durchgeführt. Dabei wird eine Software verdeckt in das informationstechnische System eingebracht, um die verschlüsselte Kommunikation „an der Quelle“ aufzuzeichnen, indem die Kommunikationsdaten vor der Verschlüsselung des abgehenden und nach der Entschlüsselung des ankommenden Datenstroms abgegriffen und gespeichert werden sollen. Analyse des Zielsystems, Aufbringung, Verschlüsselung und Ausleitung der Daten sowie anschließende Löschung funktionieren nach den technischen Prinzipien der Online-Durchsuchungs-Software[97] mit dem Unterschied, dass die Quellen-TKÜ auf die Analyse von Telekommunikationsdaten beschränkt sein soll.

Generell wird die Bezeichnung *Quellen-TKÜ* in dieser Arbeit für die Maßnahme im rechtlichen Sinne verwendet, wobei der Begriff *Quellen-TKÜ-Software* wiederum auf das konzeptionell prototypische Modell der für die Maßnahme verwendeten Software verweist. In Zitaten ist jedoch mit „Quellen-TKÜ-Software“ stets eine konkrete Implementation gemeint, doch dieser Bedeutungswechsel wird immer aus dem Kontext klar.

Da die ODS-basierte Online-Durchsuchung Medienberichten zufolge am meisten benutzt wurde,[98] wird sie in dieser Arbeit als „Standard-Online-Durchsuchung“ untersucht, um die tatsächlichen und möglichen Konsequenzen ihres Einsatzes abzuschätzen.

3 Die Online-Durchsuchung en detail

Da es keine öffentliche, detaillierte Beschreibung der konzeptionellen Anforderungen an eine heimliche Online-Durchsuchung gibt, folgt eine Konstruktion dieser Spezifikationen aus Forderungen von Politikern und anderen am Diskurs beteiligten Personen. Diese umfasst Zitate, Beantwortungen von Kleinen und Großen Anfragen an die verantwortlichen Stellen der Exekutive und Interviews. Wo dennoch entscheidende Lücken in den Anforderungen klaffen, werden aus dem rechtlichen, technischen und gesellschaftlichen Kontext sinnvolle Arbeitshypothesen abgeleitet und verwendet.
Im Folgenden werden die Grundfunktionen der Online-Durchsuchungs-Software konstruiert[99] und analysiert, wobei die entstehenden konkret technischen Problematiken direkt behandelt werden. Darüber hinausgehende informationstechnisch-konzeptionelle und gesellschaftliche

[96] Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Vorbemerkung.
[97] Bundesregierung der 16. Wahlperiode, *Drucksache 16/6535*, 28.9.2007, Antwort auf Frage 14.
[98] Patalong, *Behörden spähten 100-mal Computer aus.*
[99] Siehe Unterabschnitt 2.1 (Methodik der Arbeit).

Folgen und Probleme werden weiter unten in Abschnitt 4 (Technisch-konzeptionelle und gesellschaftliche Folgen der Online-Durchsuchung) behandelt.

3.1 Analyse der Funktionen und des Lebenszyklus der Online-Durchsuchungs-Software (ODS)

Der Übersichtlichkeit halber erfolgt die Konstruktion der konzeptionellen Anforderungen entlang des Softwarelebenszyklus, angefangen bei der Analyse des Zielsystems, weiter bei der Erstellung der Software, dann Installation im Zielsystem, über die Datensuche und Übermittlung der Funde bis hin zur Deinstallation.[100] Im Anschluss werden mögliche Fehlerszenarien betrachtet.

3.1.1 Analyse des Zielsystems

Von Privatpersonen verwendete informationstechnische Systeme wie Personal Computer, Laptops oder Mobiltelefone unterscheiden sich in den für eine heimliche Online-Durchsuchung wichtigen Aspekten stark. Sie differieren in installierten Hardwarekomponenten, installierten Softwarekomponenten sowie Versionen der installierten Software- und Hardwarekomponenten. Dies umfasst sowohl installierte Programmbibliotheken als auch die Firmware der Hardwarekomponenten. Programme, die für eine bestimmte Konfiguration geschrieben und kompiliert worden sind, funktionieren oft gar nicht, eingeschränkt oder unzuverlässig in anderen Konfigurationen.[101] Durch die später begründete notwendige Betriebssystemnähe und den notwendigen Eingriff in andere Programme muss die Online-Durchsuchungs-Software individuell auf das zu infiltrierende System zugeschnitten werden.
Wie die konkrete Konfiguration des Zielsystems ermittelt wird, ist eine vordergründig verfahrensmethodische und rechtliche Frage. Möglich wäre z. B. die Fernanalyse über das Internet. Diese Frage wird jedoch in dieser Arbeit nicht weiter vertieft.

3.1.2 Erstellung der Online-Durchsuchungs-Software

Wenn die Details des Zielsystems in Erfahrung gebracht worden sind, muss die Online-Durchsuchungs-Software für die gegebene Systemkonfiguration und die Erkenntnisanforderungen erstellt werden. Entweder wird die Software jeweils nach den Vorgaben des aktuellen Falles neu geschrieben[102] oder — was wahrscheinlicher ist — aus vorhandenen, früher erstellten Modulen neu zusammengesetzt und angepasst. Denkbare Modulklassen wären einerseits Installationsmodule, die die Sicherheitsvorkehrungen des anzugreifenden Systems umgehen und sich so Zugang verschaffen und andererseits Überwachungs-, Such- und Übermittlungsmodule, die nachgeladen werden können, wenn der Zugang erfolgreich hergestellt worden ist. Des Weiteren sollte eine „Analyse der ODS (Disassembling) [...] jedoch durch die Verwendung kryp-

[100] Vergleiche auch Hansen und Krause, *Heimliche Online-Durchsuchung – Wie geht's, wie schütze ich mich?*, 2007, Seite 15 ff.
[101] Freiling, *Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, 27.9.2007, Seite 6.
[102] Krasemann und Ziercke, *Interview u. a. zur Online-Durchsuchung*, 2007, Minute 2:35.

tographischer Methoden nahezu unmöglich gemacht“[103] werden, was neben der erschwerten Analysierbarkeit des Binärcodes auch die exakte Programmsignatur, nach der Antivirensoftware suchen könnte, verschleiert.[104] Andererseits zieht verschlüsselter Programmcode generell die Aufmerksamkeit von Viren- und Malwarescannerheuristiken auf sich; hier ist bei der Erstellung eine Entscheidung zu treffen.

Testphase

Die ODS muss für jedes Zielsystem gemäß der Analyse speziell zugeschnitten werden. Weil das Zielsystem jedoch nicht zur Verfügung steht und die ODS meist unter Zeitdruck geschrieben werden würde, ist eine ausgiebige Testphase nicht zu erwarten. Gerade bei Software, die sich so tief im System verankert und teilweise Gerätetreiber kontrollieren wird, ist ein ausgereiftes Ergebnis nötig, doch unter diesen Umständen nicht wahrscheinlich.[105]
Wenn die ODS für jeden Einsatz komplett neu erstellt werden würde,[106] müssten jeweils auch die Tests neu durchgeführt werden. Dies würde die Codequalität stark negativ beeinflussen. Bei der (Wieder-)Verwendung von Modulen wird die Fehleranfälligkeit aufgrund der mehrfachen praktischen Anwendung möglicherweise geringer, doch auch in diesem Fall können Tests nicht direkt auf dem Zielsystem unter Beachtung der installierten Softwareversionen, eventueller Wechselwirkungen und des Nutzerverhaltens durchgeführt werden.

3.1.3 Einbringung ins Zielsystem / Infiltration

Nun muss die Online-Durchsuchungs-Software in das Zielsystem eingebracht werden, wofür es drei Angriffspunkte mit jeweils verschiedenen Möglichkeiten gibt.[107]

Direkte Installation durch Dritte Der technisch einfachste und sicherste Weg ist die direkte Installation auf dem Gerät. Wie sich die ausforschende Stelle Zugriff auf das Gerät verschafft, ist auch hier eine vordergründig verfahrensmethodische und rechtliche Frage. Denkbar wären heimliche Hausdurchsuchung,[108] heimliches Aufspielen bei normaler Hausdurchsuchung, die temporäre Entwendung des Geräts,[109] Aufbringung während einer Reparatur oder durch eine Vertrauensperson,[110] jedoch ist dies nicht Gegenstand der vorliegenden Arbeit. Um die Software ohne Ausnutzung von Sicherheitslücken zu installieren, muss das Gerät entweder 1) in laufendem Betrieb mit Administratorenrechten bzw. in diesen Zustand versetzbar (per automatischem Login) oder 2) unverschlüsselt vorgefunden werden. Im ersten Fall kann die Software

[103] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort zu Frage 31.
[104] Tanenbaum, *Modern operating systems*, 2008, Seite 696.
[105] Bogk (Chaos Computer Club), *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007, Seite 16.
[106] Krasemann und Ziercke, *Interview u. a. zur Online-Durchsuchung*, 2007, Minute 2:35.
[107] Vergleiche Pfitzmann, *Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft*, 26.9.2007, Seite 5.
[108] Für Kritik an der geheimen Hausdurchsuchung für solche Zwecke laut BKA-Gesetz siehe Roggan, „Legalisierung im Polizei- und Geheimdienstrecht“, 2008, Seite 115.
[109] Mühlbauer, *Wo und wie der Bayerntrojaner zum Einsatz kommt*, 3.3.2011.
[110] Borchers und Bager, *Bürgerrechtler diskutieren mit BKA-Chef über Online-Durchsuchung*, 22.9.2007.

von einem zugreifbaren Speichermedium (z. B. USB-Stick oder über das Internet) geladen und normal installiert werden. Im zweiten Fall muss man mit einem fremden System direkt auf den Datenträger zugreifen und die Software ohne die üblichen Installationsroutinen im Zielsystem verankern. Beide Wege sind praktisch sehr schwierig zu begehen, da ersterer sehr unwahrscheinlich und letzterer als technisch anspruchsvoll einzustufen ist, da die für die Heimlichkeit notwendige Kompatibilität mit dem Rest des Systems sichergestellt werden muss. Allerdings kann der erste Fall durch externe Faktoren herbeigeführt werden, z. B. „erweiterte" Flughafenkontrolle oder die oben benannte offene Hausdurchsuchung..

Direkte Installation durch den Betroffenen Nicht zu vernachlässigen ist die Möglichkeit der Installation durch den Betroffenen selbst. Dabei wird er unwissentlich dazu gebracht, die ODS eigenhändig in das System zu bringen; er wird schlicht überlistet.[111]
Verfahren, um dies zu erreichen, basieren in der Regel auf der Ausnutzung des Vertrauens[112] oder der Neugier des Betroffenen.[113] Das Vertrauen kann sich auf Personen beziehen, von denen er z. B. eine Mail mit Anhang bzw. einem Link bekommt, den er öffnen soll, oder aber Vertrauen in das informationstechnische System selbst, das ihm z. B. eine Datei als (sicheres) Dokument präsentiert, obwohl es sich tatsächlich um ein (unsicheres,) ausführbares Programm handelt. Aufschlussreiches Beispiel ist folgende Benennung für ein Windowsprogramm: „Dokument.pdf.exe". Wenn der verwendete Dateimanager standardmäßig die Dateiendung ausblendet, wird nur „Dokument.pdf" angezeigt. Soll das vermeintliche Dokument geöffnet werden, wird tatsächlich das Programm ausgeführt. Im Kontext einer Nachricht einer vermeintlich berechtigten Stelle, die für einen notwendigen Vorgang das Öffnen des Anhangs empfiehlt, z. B. vermeintliche Abmahnungen mit den Vorwürfen im Anhang, sind die Erfolgsaussichten einer solchen Installation gut.
Die Neugier bezieht sich dagegen auf Postwurf-Werbe-CDs, SD-Karten an Abschlussarbeiten oder vermeintlich verlorene und durch die Zielperson gefundene Datenträger mit unbekanntem Inhalt, der inspiziert werden möchte.[114] Hier greifen entweder soeben beschriebene Verfahren oder die weiter unten beschriebene Ausnutzung von Sicherheitslücken.
Es muss sichergestellt werden, dass der Nutzer diese Dateien/Datenträger auf seinem, dem Zielsystem, öffnet, ansonsten würde das falsche System infiltriert.

Manipulation (an) der Netzinfrastruktur Ein weiterer Weg besteht in der Manipulation der Netzwerkdatenströme auf dem Weg zum Zielsystem. Auch hier sind die rechtlichen Probleme, den Datenstrom zwischen zwei Kommunikationspartnern an Netzknoten abzufangen und zu manipulieren, vielschichtig, aber nicht Gegenstand dieser Arbeit. Auch technisch gestaltet sich dies schwierig, weil Betriebssystemhersteller wie Microsoft, Apple, Google und auch die Anbieter von Linux-Distributionen ihre Softwareupdates signieren und so gegen externe

[111] Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seite 13 siehe auch Eikenberg, *Microsoft-Bericht: Fast die Hälfte der Anwender infiziert ihre Rechner selbst*, 13.10.2011.
[112] Vertrauen hier als Möglichkeit der Kompensation informationeller Unsicherheit, also als Handlungsmöglichkeit trotz fehlenden Wissens. Siehe dazu Kuhlen, *Die Konsequenzen von Informationsassistenten*, 1999, S.12.
[113] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort auf Frage 38.
[114] Vergleiche Hansen und Krause, *Heimliche Online-Durchsuchung – Wie geht's, wie schütze ich mich?*, 2007.

Veränderung schützen. Lediglich technisch ungeschützte Datenströme — Klartextdaten oder unzureichend verschlüsselte Daten, die sich mit kryptographischen Angriffen entschlüsseln und verändern lassen — könnten mit hohem Aufwand so verändert werden, dass sie in der Folge die ODS zum Zielsystem mittransportieren. Darüber hinaus muss ein Datenstrom gewählt werden, der im Zielsystem in der Art verarbeitet wird, dass dadurch die ODS installiert wird. Eine solche Einbringung basiert jedoch nicht auf der Ausnutzung von Sicherheitslücken im System.
Generell ist das Internet ein auf Paketvermittlung basierendes Netzwerk, daher ist der Datenweg einer Übertragung innerhalb des Netzes sehr schwer bis gar nicht vorhersehbar. Eine für diese Aufbringungsmethode nutzbare Ausnahme bilden Internetprovider, da jeglicher Datenverkehr ihrer Kunden über die Providerinfrastruktur abgewickelt wird. Unter Mitwirkung desjenigen Internetproviders, der den Internetzugang des Zielsystems bereitstellt, kann der gesamte Datenstrom des Zielsystems mit dem Internet abgefangen und verändert werden.

Zusammenarbeit mit Softwareherstellern Technisch denkbar wäre auch die Möglichkeit, mit Softwareherstellern zusammenzuarbeiten. So könnten in deren Produkte Mechanismen eingearbeitet werden, mithilfe derer die befugten Behörden auf Zielsysteme zugreifen könnten. Diese Möglichkeit wurde jedoch politisch verworfen; „Absprachen mit Herstellern von Software werden dabei nicht angestrebt“,[115] weil „absichtlich eingebaute Schwachstellen in Soft- und Hardware [...] nicht nur für die IT-Sicherheit, sondern auch für die deutsche IT-Wirtschaft fatale Konsequenzen“[116] hätten.

Ausnutzung von Sicherheitslücken im informationstechnischen System Eine andere Art, die ODS in ein informationstechnisches System zu bringen, besteht in der Ausnutzung von Sicherheitslücken. Dies erfolgt in zwei Schritten: Erstens muss eine entsprechend verwendbare Sicherheitslücke im Zielsystem in Erfahrung gebracht werden und zweitens muss die ODS so modifiziert werden, dass sie diese Sicherheitslücke tatsächlich ausnutzen kann (ein sogenannter Exploit). Woher die zu verwendenden Sicherheitslücken stammen sollen, wurde öffentlich nicht weiter diskutiert. Zwar war der Ankauf dieser Exploits für normale Behörden nicht geplant,[117] dafür agierte der Bundesnachrichtendienst als Amtshilfe bei der Durchführung von Online-Durchsuchungen mit Hilfe erwähnter, eingekaufter Exploits.[118]

Es gibt eine Vielzahl möglicher Sicherheitslücken: Von Fehlern oder unvorhergesehenem Verhalten des Betriebssystems und dessen Peripherie (z. B. Netzwerkstack) bis hin zu auf dem Zielsystem installieren Anwendungen. Dabei ist die Angriffsfläche auf heutigen Personal Computern potenziell eher groß, da oft viele Anwendungen installiert und genutzt werden, die Netzwerkfunktionalität besitzen oder auf extern zugeführten Daten arbeiten: Angefangen bei Web-

[115] Bundesregierung der 16. Wahlperiode, *Drucksache 16/4997*, 10.4.2007, Antwort zu Frage 4.
[116] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort zu Frage 9.
[117] A.a.O. Antwort auf Frage 43.
[118] Sieber, *Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen*, 9.10.2007, Seite 11.

browsern, die präparierte Webseiten als Einfallstor ermöglichen,[119] über E-Mailprogramme, die manipulierte E-Mails falsch verarbeiten, so dass fremder Code ausgeführt werden kann,[120] weiter zu fehlerbehafteter Dokumentenlesesoftware, die bei vorbereiteten Dokumenten ungewollt Codeausführung ermöglicht,[121] bis hin zu direkten Angriffen auf das Betriebssystem von Rechnern, die mit dem Internet verbunden sind.[122]

Für einen Remoteangriff über das Internet ist zumindest die IP-Adresse des Zielsystems nötig. Durch die überwiegende Nutzung des Internets über Personal-Router mit Firewalls und Network Address Translation (NAT) haben private Systeme jedoch nur noch selten eine eigene Internet-IP-Adresse und sind daher auch nicht von „außen“ direkt ansprechbar.[123] Selbst die IP-Adresse eines privaten Internetanschlusses ist nicht statisch und wechselt mindestens aller 24 Stunden aufgrund der nach dieser Verbindungsdauer üblichen Zwangstrennung bei deutschen Providern. Auch für mobile Endgeräte gilt diese Zielschwierigkeit, weil Mobilfunkprovider für mobiles Internet fast gänzlich NAT-Adressen vergeben. Diese Problematik stellt ein fast unlösbares Problem dieser Methode dar, siehe auch Abschnitt 3.3 (Falsches System infiltriert).

Im Falle des für den Angreifer positiven Ausgangs der Infiltration erlangt die ODS Zugriff zum System und hat sich dort installiert/verankert. Die Verankerung ist ein komplexer Vorgang und wird im nächsten Teil detailliert erläutert.

3.1.4 Verankerung im System

Um die Verankerung der ODS in einem informationstechnischen System zu verstehen, ist es nötig, einige Grundlagen digitaler Computer zu erklären. Nur so können die Anforderungen, Funktionen und Fähigkeiten der Software verstanden und eingeordnet werden.

Das Betriebssystem eines Computers erfüllt hauptsächlich zwei Funktionen. Einerseits stellt es Programmen eine Abstraktion der konkreten Hardware zur Verfügung und andererseits verwaltet es vorhandene Ressourcen. Diese umfassen Prozessor(en), Arbeitsspeicher, Ein- und Ausgabegeräte, externe Speicher, Timer und Netzwerkkomponenten, so dass z. B. mehrere Programme gleichzeitig laufen können, ohne sich mehr als nötig zu behindern.[124] Die Verwaltungsfunktion ist gleichzeitig Kontrollfunktion und umfasst den Schutz der Integrität von Anwendungsprogrammen und des Betriebssystems selbst.

---

[119] Auf diese Art wurde z. B. der *Computer and internet protocol address verifier (CIPAV)*, das ODS-Pendant des FBI, in den USA auf den Computern der Betroffenen installiert Poulsen, *Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years*, 16.4.2009.

[120] Siehe z. B. *Bagle.Q*-Wurm, der die Verarbeitung von HTML-E-Mails angreift.

[121] Laut Studie der CSIS Security Group A/S ist z. B. der Adobe Reader für 32% der Infektionen verantwortlich ‚Kruse, *This is how Windows get infected with malware*, 27.9.2011.

[122] Siehe *Sasser*-Wurm von 2004, der bestimmte Windowsversionen direkt vom Internet aus infiltrieren kann.

[123] Im Detail beschrieben bei Chaos Computer Club, *QUELLEN-TKÜ-Stellungnahme des Chaos Computer Clubs*, 2009, Seite 15 ff.

[124] Tanenbaum, *Modern operating systems*, 2008, Seiten 4 bis 6 und Silberschatz, Galvin und Gagneand, *Operating System Concepts*, 2009, Seite 5.

Um größtmögliche Heimlichkeit zu erreichen — also vom Benutzer des informationstechnischen Systems unbemerkt agieren zu können, muss die ODS sich tief im Betriebssystem verankern. Dies zu erklären, erfordert die Betrachtung zweier Konzepte von Betriebssystemen.

Rechtekonzept

Moderne Betriebssysteme nutzen zum Schutz der Integrität des Systems ein je nach Ausgestaltung mehr oder weniger ausdifferenziertes Rechte- oder Privilegiensystem. In diesem Paradigma werden Prozessen (z. B. laufenden Anwendungen) bei der Ausführung bestimmte Privilegien zugewiesen, die sich grob in Kernelmode- und Usermodeprivilegien[125] unterteilen lassen, wobei Prozesse im Usermode sehr wenig und im Kernelmode maximal privilegiert sind.
Die in der Informatik übliche, exakte Unterteilung in fünf Privilegienringe (Usermode als Ring 3 bis Hypervisormode als Ring -1) ist für unsere Betrachtung der gängigen Personalcomputerbetriebssysteme (Windows/Mac OSX/GNU-Linux) nicht von Belang, daher wird dieser Sachverhalt hier hinreichend vereinfacht dargestellt.[126]

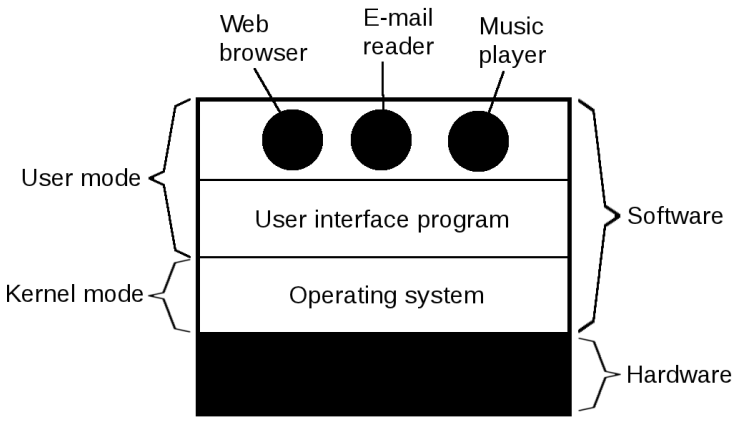


Abbildung 1: Privilegienprinzip eines Computersystems (aus Tanenbaum, *Modern operating systems*, 2008, Seite 2)

Im Usermode laufende Prozesse haben einen stark beschränkten Zugriff auf Systemhardware und im System gespeicherte Daten, sie müssen den Zugriff darauf beim Betriebssystem „erfragen“. Unter Beachtung von Sicherheitsrichtlinien werden die Ressourcen dann zur Verfügung gestellt oder auch nicht. Sicherheitsrichtlinien für Datenzugriffe werden mit dem Konzept der Rechteidentitäten umgesetzt. Rechteidentitäten werden gemeinhin (nicht ganz korrekt) mit Benutzern gleichgesetzt, üblich ist auch der Terminus „Benutzerkonto“. Verschiedene Betriebssysteme gehen dieses Konzept im Detail verschieden an, aber die Unterschiede sind für den Kontext dieser Arbeit nicht von Bedeutung.

[125] Tanenbaum, *Modern operating systems*, 2008, Seite 2.
[126] Siehe dazu A.a.O. Seite 247.

Einerseits hat jeder Prozess eine bestimmte Rechteidentität und andererseits wird Daten (z. B. Dateien) explizit zugewiesen, welche Rechteidentität welchen Zugriff darauf hat.[127] Wird ein Prozess gestartet, erbt er die Rechteidentität des ihn startenden Prozesses. Eine vom Nutzer gestartete Anwendung kann also ihrerseits nur Programme mit den gleichen Rechten, denen des Nutzers, starten. Browser, Bildbearbeitungsprogramme und Musikabspielsoftware laufen z. B. in diesem Modus.

Im Kernelmode laufende Prozesse haben unbeschränkten Hardware- und Datenzugriff, sie haben die gleichen Rechte wie der Betriebssystemkern selbst. Kernelmodule, Firewalls und Gerätetreiber z. B. müssen zwangsläufig in diesem Modus laufen.[128] Als Konsequenz dieser Privilegierung können von derartigen Prozessen ungeachtet einer Rechteidentität beliebige Daten erstellt, verändert und gelöscht werden. Hierbei spricht man auch von Administrator-, Superuser- oder Rootrechten (Engl. *root*: Wurzel/Ursprung).

Dateikonzept

Daten auf Speichermedien werden in modernen Betriebssystemen in Dateien organisiert.[129] Eine Datei ist ein abstraktes Konzept eines Behälters für Daten, wobei Dateien in Dateisystemen organisiert werden. Die konkrete Implementation des Dateisystemkonzeptes variiert je nach Betriebssystem, Datenträger und Nutzerkonfiguration, spielt aber für die Belange dieser Arbeit nur eine untergeordnete Rolle. Von Bedeutung sind konzeptionelle Eigenschaften, die allen Dateisystemen gemein sind, insbesondere das Metadatenkonzept.[130]

In Dateien werden nicht nur die zu speichernden Daten selbst vorgehalten, sondern auch Informationen über die Daten und Eigenschaften des speichernden Dateikonstruktes, sogenannte Metadaten oder Metainformationen. In diesen Metadaten kann enthalten sein, wer — welche Rechteidentität — der Besitzer der Datei ist, wer die Datei erstellt hat, wann sie erstellt wurde, wer welche Zugriffsrechte hat, wann sie zuletzt gelesen oder verändert wurde und vieles mehr, das nicht aus den gespeicherten Daten hervorgeht.[131] Gerade weil diese Informationen, z. B. der Besitzer der Datei, nicht aus den gespeicherten Daten an sich ableitbar sind, müssen sie zusätzlich gespeichert werden, es handelt sich daher um *extrinsische* Informationen über die gespeicherten Daten. Die üblicherweise in Computern verwendeten Dateisysteme („NTFS“ in Microsofts Windows, „ext3/4“ in GNU/Linux und „HFS+“ in Apples Mac OS X) speichern mindestens die eben genannten Informationen.

Anmerkung: Das Metadatenkonzept ist ineinander verschachtelbar, so können die in einer Datei gespeicherten Daten, z. B. eine Fotodatei wiederum aus Daten (reine Bilddaten) und Metadaten (Kameramodell, Aufnahmedatum etc.) bestehen.

[127] Siehe Abschnitt 3.1.4 (Dateikonzept).
[128] Microkernelarchitekturen stellen eine seltene Ausnahme dar und werden hier nicht berücksichtigt.
[129] Tanenbaum, *Modern operating systems*, 2008, Seite 257.
[130] A.a.O. Seite 263.
[131] A.a.O. Seite 263.

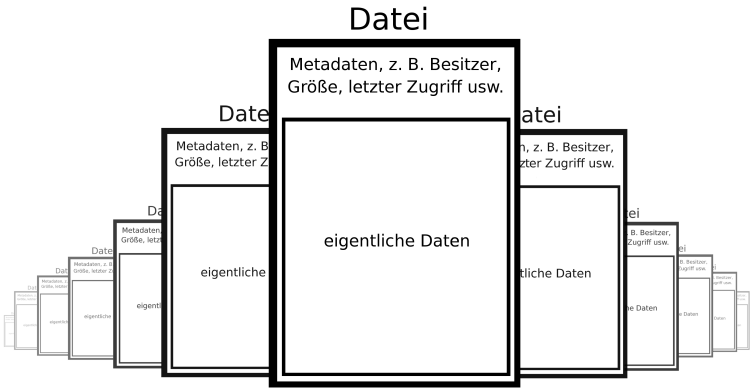


Abbildung 2: Vereinfachte Dateistruktur: Eine Datei umfasst viele Metadaten

Lese- und Schreibrechte für Nutzerdaten, Usermode

Sinnvoll für normale Systemdaten sind Nur-Lese-Rechte für alle Standardrechteidentitäten und zusätzlich Schreibrechte für das Betriebssystem oder Teilprogramme davon. Benutzerdaten haben Lese- und Schreibrechte für den Benutzer selbst und eventuell Leserechte für andere Rechteidentitäten. An dieser Stelle sei angemerkt: Sinn dieses Rechte-/ Privilegiensystems ist nicht der Schutz der Privatsphäre eines Benutzers, sondern allein die Bewahrung der Konsistenz und Sicherheit des Systems an sich.
Es ist klar ersichtlich, dass Leserechte zum Durchsuchen und Kopieren von Daten nötig sind. Wenn die auf einem System gespeicherten Benutzerdaten globale Leserechte haben, ist dies zudem sehr einfach mit beliebigen Rechteidentitäten zu gewährleisten.
Da die üblicherweise in Computern verwendeten Dateisysteme — wie weiter oben beschrieben — in den Metadaten jeder Datei protokollieren, wann zuletzt lesend auf sie zugegriffen wurde, ändert ein Durchsuchen von Daten kontinuierlich die Dateisysteminformationen. Um möglichst keine Spuren des Suchens zu hinterlassen, weil dies die Heimlichkeit gefährden würde, muss die ODS diese Metainformationen von Dateien nach jedem Datenzugriff auf den vorherigen Wert zurücksetzen. Sie benötigt daher nicht nur Leserechte, sondern auch Schreibrechte für die Daten des Benutzers.
Die notwendigen Lese- und Schreibrechte für die Suche in Nutzerdaten sind gewährleistet, wenn die ODS im Usermode und der Rechteidentität des Nutzers laufen kann, als gering privilegiertes Programm.

Die Online-Durchsuchungs-Software im Kernelmode

Das Betriebssystem hat aufgrund der Verwaltungsfunktion zwangsläufig Kenntnis von allen laufenden Programmen, ihrer Ressourcennutzung und anderen Zustandsinformationen. Diese Statusdaten des Systems sind grundsätzlich von jeder normalen Rechteidentität abrufbar; bei Microsofts Windows z. B. mit dem Programm „Taskmanager“, bei Apples Mac OS X z. B. mit dem Programm „Aktivitätsmonitor“ und bei GNU/Linux z. B. mit dem Programm „top“.

Auch die Online-Durchsuchungs-Software und ihre Aktivitäten sind dort erfasst, leicht auffindbar für Nutzer des Systems und Software, die anormale Systemaktivität finden soll.

Damit das „Entdeckungsrisiko eines solchen Programms (der ODS, Amn. d. Verfassers) gering einzustufen ist“,[132] muss es seine Existenz auf dem System des Betroffenen verbergen. Es muss daher z. B. Anfragen nach Prozessstatusinformationen abfangen und verändern können, um sich selbst aus Prozessauflistungen und Berichten zu entfernen. Dazu muss es sich zwischen die abfragenden Applikationen und das antwortende Betriebssystem schalten, sogenanntes Hooking. Das ist Programmen im Usermode nur mit anderen Usermodeprogrammen möglich.[133] Beim Betriebssystem selbst ist dies als Usermodeprogramm jedoch sehr schwer bis gar nicht machbar,[134] daher sollte die ODS zumindest teilweise im Kernelmode laufen, auch um die eigenen Dateisystemaktivitäten (Änderungen an Metadaten, Speicherung der Funde etc.) aus dem Dateisystemlogbuch, dem sogenannten Journal, zu löschen.

Doch auch wenn der Benutzer nicht dauerhaft den Zustand seines Systems überwacht, kann installierte Abwehrsoftware die ODS und ihre Aktivitäten aufspüren und melden. Software für die Entfernung von Spyware und Malware sowie Firewalls und Antivirenprogramme werden immer häufiger auch auf privaten Systemen eingesetzt[135] und sind in der aktuellen Version des am weitesten verbreiteten Betriebssystems Microsoft Windows schon vorinstalliert. Eine weitergehende Absicherung des Systems durch Intrusion-Detection-Systeme (IDS) ist zusätzlich denkbar.

Da es „nicht vorgesehen (ist), die auf dem System befindlichen Sicherheitssysteme auszuschalten“,[136] muss die ODS auch diese Programme täuschen oder umgehen. Die oben genannte Abwehrsoftware arbeitet nur dann fehlerfrei, wenn die von ihr zu überwachende Software nicht auch im Kernelmode arbeitet.[137] Auch aus diesem Grund sollte die ODS zumindest teilweise im Kernelmode laufen.

Zusätzlich kann nur eine im Kernelmode agierende ODS uneingeschränkt auf jegliche Daten des Systems zugreifen, egal ob Nutzer- oder Systemdaten. Dies ist generell nötig, um auch auf beliebige, „flüchtige, das heißt nur im Arbeitsspeicher des Rechners befindliche [...] Dateien“[138] wie Passwörter o. ä. zugreifen zu können.

Folglich sollte das Kernelmodeprivileg so früh wie möglich erlangt werden, bestenfalls bei der Einbringung ins System oder — falls im konkreten Fall nicht anders möglich — später, auch wenn damit die Datensuche nur eingeschränkt möglich ist und eine Entdeckung wahrscheinlicher wird.

---

[132] Bundesregierung der 16. Wahlperiode, *Drucksache 16/4997*, 10.4.2007, Antwort zu Frage 5.

[133] Siehe Werner, *Federal Trojan's got a "Big Brother"*, 18.10.2011.

[134] Weiterführend siehe z. B. Mxatone und IvanLeFou, „Stealth Hooking: another way to subvert the Windows kernel“.

[135] Laut Symantec-Studie haben 80% der Privatnutzer aktualisierte Antispyware und Antivirussoftware, Kaiser, *Small and Midsized Businesses Aware of Security Risks, But Not Doing All They Can to Protect Information.*

[136] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort auf Frage 19.

[137] Tanenbaum, *Modern operating systems*, 2008, Seite 698 ff.

[138] Bundesregierung der 16. Wahlperiode, *Drucksache 16/4997*, 10.4.2007, Antwort zu Frage 13.

Dass die ODS im Kernelmode agiert und uneingeschränkte Rechte besitzt, heißt jedoch nicht, dass sie auch uneingeschränkt Kontrolle auf das System ausüben kann. Sie ist immer noch auf einem fremden System zusammen mit dem Betriebssystem und anderen Programmen des Betroffenen, die sehr wahrscheinlich nichts von der ODS „wissen“. Wie diese Umgebung die Aktivitäten der ODS interpretiert und darauf gegebenenfalls reagiert, ist nicht vorhersehbar. Dieser Umstand wird später nochmals wichtig werden, wenn es um die Interpretation der Datenfunde geht.

3.1.5 Update der Software

Wegen der schnellen Updatezyklen heutiger Software, der tiefen Verwurzelung in System und Software muss auch die ODS regelmäßig aktualisiert werden.[139] Dabei muss der aktualisierte Code entweder aktiv von der ODS abgefragt, heruntergeladen und installiert werden (pull) oder das Update vom ODS-Kontrollzentrum der ausführenden Behörde zu gegebener Zeit initiiert werden (push). Es ist für die ODS zweckmäßig und sinnvoll, regelmäßig aktiv nach Updates zu suchen, weil das System von „außen“ vermutlich oft nicht erreichbar sein wird[140] und die Erreichbarkeitsfunktion der ODS auch nicht in Planung ist.[141]

Updates sollen Funktionalitäten von Software ändern. Das kann der Fehlerbeseitigung dienen, aber auch der Herstellung von Kompatibilität, der Erweiterung der Funktionalität oder der Neukonfiguration bestehender Komponenten.

Bei einem Update werden Teile der installierten Software erweitert, ersetzt, verändert oder gelöscht. Die Updateroutine (ein eigenes Programm) führt dabei die Änderungen durch, sie muss die ODS-Programmdaten, aber auch Systemdaten ändern, um gegebenenfalls neue Komponenten zu registrieren, vorhandene zu aktualisieren oder zu deregistrieren. Updates können von kleinen Änderungen wie bytegroßen Bugfixes über mittlere Änderungen, wie z. B. die Anpassung an eine neue Browserversion, bis zu wesentlichen Änderungen wie der Installation einer komplett neuen Software, eines neuen Gerätetreibers oder ähnlichem reichen.

Üblicherweise führen Updates vor und nach dem eigentlichen Updatevorgang weitere Aktionen aus. Vor dem Updatevorgang werden üblicherweise Programmversion und Konsistenz der Daten überprüft sowie das zu aktualisierende Programm beendet, nach dem Updatevorgang werden üblicherweise temporäre Dateien, die nur für das Update angelegt worden sind, entfernt sowie die neue Version der Software gestartet.

Nach diesen Schritten ist die ODS im System verankert und kann ihre vor dem Anwender zu versteckende Arbeit aufnehmen. Abschließend muss angemerkt werden, dass bei der Nutzung eines Nur-Lese-Medium-basierten Betriebssystem die Einbringung der ODS in das Zielsystem durch jeden Neustart rückgängig gemacht wird. Livesysteme verschiedener GNU/Linuxdistributionen sind dafür geeignet, wenn sie z. B. von CD/DVD gestartet werden.

---

[139] dapd/dpa, *Minister mokiert sich über Chaos Computer Club*, 16.10.2011.

[140] Siehe Unterabschnitt 3.1.3 (Einbringung ins Zielsystem / Infiltration).

[141] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort auf Frage 6.

3.1.6 Datensuche

Mit den erforderlichen Rechten kann die ODS nun auf dem System nach „ermittlungsrelevanten Informationen“[142] suchen. Da sie im Kernelmode läuft, hat sie wie oben beschrieben die Möglichkeit, jegliche Datenquellen anzuzapfen, sei es Bildschirminhalt, Tastenanschläge, Daten auf Speichermedien, Netzwerkverkehr, Kamera- und Mikrofondaten, Mausbewegungen, verbundene Netzlaufwerke oder Druckaufträge bis hin zu den Namen verwendeter Drahtlosnetzwerke. Bis jetzt politisch im Gespräch waren noch hauptsächlich Festplatten und andere Permanentspeicher[143] sowie neuerdings auch Bildschirminhalte.[144]

Auf Speichermedien überhaupt nach Inhalten zu suchen ist insofern nötig, als dass eine regelmäßige Komplettübertragung aller Daten des Systems außer Frage steht[145] und auch der Wahrung des Kernbereichs privater Lebensgestaltung entgegensteht.[146] Es muss also eine Vorauswahl der zu übermittelnden Daten getroffen werden. Dies gestaltet sich prinzipiell schwierig, da nicht bekannt ist, welche Informationen dort überhaupt vorliegen. Es müssen also Annahmen darüber gemacht werden, welche Informationen vorliegen könnten und mit welchen Suchkriterien sie gefunden werden würden.[147] Zu beachten ist dabei, dass zum Schutz des Betroffenen die nicht relevanten Inhalte auch nicht gefunden werden sollen, denn die gefundenen Daten werden gesammelt, um später von anderen Personen bei der Durchsicht als relevant zur Kenntnis genommen zu werden.[148]

Es ist am sinnvollsten, nach Texten oder Textstellen zu suchen, da asynchrone Kommunikation und Fixierung von Gedanken in Computern fast immer durch Schriftnutzung realisiert werden. Hinzu kommt, dass textbasierte Informationen aufgrund des digitalen Charakters von Schriftnotationssystemen[149] prinzipiell einfach syntaktisch durchsuchbar sind. Hierunter fallen auch Tondaten mit gesprochenem Inhalt, wenn sie mit Spracherkennung in Textinformationen umgewandelt werden können.

Für andere Medien wie Bild-, Video- und sonstige Tondaten ist eine sinnvolle Suche momentan ungleich schwieriger bis unmöglich; einerseits technisch, weil derartige Suchalgorithmen noch in den Kinderschuhen stecken,[150] und anderseits repräsentationell, denn die formalisierte, symbolische Abstraktion der Sprache (Beispiele: „Waffe“, „Gefahr“, „Ort“, „Tat“) fehlt visuellen/auditiven Darstellungen gänzlich.[151]

Für die Suche sind folgende kombinierbare Vektoren möglich und angedacht:[152]

---

[142] A.a.O. Antwort zu Frage 2.

[143] A.a.O. Antwort zu Frage 2.

[144] Siehe Tabelle 1.2 (Einordnung des Problems).

[145] Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seite 14.

[146] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum großen Lauschangriff*, 3.3.2004, Leitsatz 2.

[147] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort zu Frage 5.

[148] A.a.O. Antwort zu Frage 2.

[149] Vergleiche Goodman, *Languages of Art*, 1976, Ende Kapitel IV.

[150] Bogk (Chaos Computer Club), *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007, Seite 15.

[151] Vergleiche Goodman, *Languages of Art*, 1976, Kapitel IV.

[152] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort auf Frage 7 und Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seite 6.

Stichwortsuche in Texten Nach Festlegung der relevanten und wahrscheinlich genutzten Worte oder Wortfolgen durch die verantwortlichen Stellen kann die ODS in den Daten danach suchen. Präzisiert werden kann die Suche durch Kombination der Suchterme mit den logischen Operatoren UND, ODER, NICHT sowie durch die Nutzung von regulären Ausdrücken, Maskierung mit Jokerzeichen und Nutzung der Methoden unscharfer Suche (Fuzzysuche), bei der auch geringe Abweichungen vom Suchterm als Treffer gelten. Metriken, die solche „Abweichungsentfernungen" erzeugen können, müssen vorher definiert werden und sind in ihrer Anwendung meist sehr rechenintensiv.

Alternativ ist es möglich, die Daten des informationstechnischen Systems von der ODS automatisch indizieren (verschlagworten) zu lassen oder bereits auf dem System existierende Indexe zu verwenden und nur den Index zu übermitteln, so dass zunächst extern darauf gesucht werden kann.

„Semantische Suche" in strukturierten Daten Sollten die Daten in semantisch-strukturierter Form vorliegen, kann auch mit den entsprechenden semantischen Methoden gesucht werden; allerdings ist die semantische Anreicherung von Daten im Grunde wieder eine rein syntaktische Zuweisung, wenn auch auf einer Metaebene. Somit kann die „Semantische Suche" konzeptionell unter der Stichwortsuche subsumiert werden.

Suche anhand von Dateinamen Neben der Suche in Dateien ist es möglich, nach bestimmten Dateinamen zu suchen. Dies kann als besonderer Teilaspekt der Stichwortsuche angesehen werden, da auch hier nach Wörtern und Wortfolgen gesucht wird, aber unabhängig vom Dateiinhalt. Die Entscheidung darüber, welches erfolgversprechende Suchworte sind, gestaltet sich hier schwieriger, weil Dateinamen meistens vieldeutig sind. Man beachte Dateinamen wie z. B. „aktion-eiscafe.jpg" und „letzter-tag-mit-euch.doc". Informationstechnisch ist diese Art der Suche sehr viel weniger ressourcenintensiv (es müssen weniger Daten durchsucht werden) und sie erfasst alle Dateitypen, andererseits sind die Ergebnisse sehr viel ungenauer.

Speicherort, Dateiformat, Datum Diese Kriteren eignen sich hauptsächlich zur Eingrenzung des Suchraumes durch Informationen, die den Kontext der gesuchten Daten beschreiben. Die explizite Angabe des Speicherortes kann sinnvoll sein, wenn anderweitig in Erfahrung gebracht wurde, dass Gesuchtes z. B. auf angeschlossenen USB-Sticks, in speziellen Verzeichnissen oder auf Netzlaufwerken gespeichert ist. Das Dateiformat kann die Suche auf eine bestimmte Art von Dateien beschränken, z. B. Klartextdateien, Verschlüsselungscontainerdateien, Suchindizes anderer Programme, Bilder oder speziell E-Maildaten. Die Einschränkung des Datums kann bei der Suche helfen, indem z. B. Dateien, die lange nicht geöffnet worden sind, nicht mit einbezogen werden oder nur in Dateien gesucht wird, die innerhalb einer bestimmten Zeitspanne geändert wurden. Hierbei muss bedacht werden, dass nicht nur das Dateisystem einige solcher Metainformationen bereithält, sondern die Dateiformate selbst auch. So beschreibt die Dateisysteminformation über das Erstellungsdatum einer Fotobilddatei nur, wann die Datei im Dateisystem angelegt wurde, nicht aber, wann das Foto gemacht wurde. Diese Information ist

in den Exif-Daten[153] des Fotos selbst zu finden. Viele Dateiformate bieten die Möglichkeit, die schon vorgesehenen Metainformationen noch zu erweitern.

Suche anhand sonstiger Metainformation Auch sonst gibt es in vielen Dateiformaten zusätzliche Metadaten. So können die oben schon erwähnten Exif-Daten auch die GPS-Positionsdaten des Ortes enthalten, wo das Foto gemacht worden ist und von welchem Kameramodell. Viele Dokumentformate hingegen speichern z. B., welcher Nutzer daran wie lange gearbeitet hat, welches Programm verwendet wurde und wo das Dokument gespeichert war.[154] Wenn es im konkreten Fall sinnvoll erscheint, kann auch nach diesen Metadaten gesucht werden.

Es ist anzumerken, dass das Suchen und Indexieren in informationstechnischen Systemen sehr ressourcenintensiv sein kann, was für den Betroffenen unter Umständen zu merklichen Leistungseinbußen und Systemreaktionsverzögerungen führen kann.

Andere Datenquellen

Noch nicht klar gesetzlich geregelt, aber technisch unter den gegebenen Umständen kein Problem ist das Anzapfen anderer Datenquellen, von denen es unzählige auf einem modernen informationstechnischen System gibt. Jedes angeschlossene Gerät kann gesteuert und abgefragt, jede Statusdatei kann ausgelesen und alle internen und externen Informationsströme können überwacht werden.[155] Im Gegensatz zu auf dem System gespeicherten Textdokumenten ist eine Filterung der so vorgefundenen Daten jedoch ungleich schwieriger, wenn nicht generell unmöglich, da keinerlei erfolgversprechende Annahmen gemacht werden können, wonach man z. B. in einem Screenshot suchen sollte. Bei der Verwendung dieser Datenquellen würden also alle erhobenen Daten gespeichert werden. Damit die Bedeutung der Tatsache, dass alle Datenquellen angezapft werden können, klarer wird, folgen einige Beispiele:

Tastenanschläge Die ODS kann alle Tastenanschläge des informationstechnischen Systems protokollieren. Das würde z. B. geschriebene Texte, E-Mails, E-Mailadressen, Passwörter, Loginnamen, Gesuchte Dateien und Terminalbefehle umfassen. Dies ist die Funktionalität eines softwarebasierte Keyloggers.

Mausbewegungen Maus- und Touchpadbewegungen, Klicks und markierte Bereiche können einfach gespeichert werden. Dies umfasst auch, wann die Maus nicht bewegt wird.

Ein- und ausgehender Netzwerkverkehr Jeglicher Netzwerkverkehr kann mitgeschnitten, gespeichert und genau analysiert werden. Das beträfe z. B. aufgerufene Webseiten, verschickte E-Mails, deren Anhänge, heruntergeladene Dateien, angeklickte Onlinevideos und

[153] Das „Exchangeable Image File Format“ ist ein weit verbreiteter Standard der JEITA für die Metadaten von digitalen Fotos, siehe Exif.org, *Exif Specifications*, 2003.

[154] Siehe Schneier, *Secrets and Lies*, 2004, Seite 32 und Bachfeld, *Verräterische Metadaten aus Web-Dokumenten extrahieren*, 26.4.2011.

[155] Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seite 7.

den Aufbau verschlüsselter Verbindungen z. B. von VPNs sowie welche Programme für die jeweiligen Datenströme verantwortlich sind.

Bildschirminhalt Der Bildschirminhalt kann abgefragt, gespeichert und verändert werden. So ist es möglich, periodisch Screenshots zu machen oder die Bildschirmausgabe gänzlich „abzufilmen".

Aktuell laufende Prozesse/installierte Programme Die Ressourcennutzung laufender Prozesse sowie die Auflistung installierter Programme sind für die ODS abrufbar, wobei diese Informationen z. B. für eine Quellen-TKÜ von Wichtigkeit sind, da sie Indizien dafür liefern können, ob gerade ein Telekommunikationsvorgang stattfindet.

Druckaufträge Die Druckerwarteschlange kann ausgelesen werden, so dass rekonstruiert werden kann, welche Dokumente, Bilder oder Daten generell wann wie oft und wo gedruckt wurden und ob der Druckauftrag erfolgreich zum Drucker übermittelt wurde.

Kamera- und Mikrofondaten Natürlich kann die ODS auch angeschlossene (Web)Kameras und Mikrofone aktivieren und so jederzeit Aufnahmen von der Umgebung machen. Die ODS besitzt folglich die Funktionen eines audiovisuellen Überwachungsmoduls (im Spionagejargon „Wanze" bezeichnet), das der Betroffene sogar selbständig auflädt. An dieser Stelle ist es wichtig, die Quellentelekommunikationsüberwachung zu erwähnen, denn die Kamera- und Mikrofondaten während eines Telekommunikationsvorganges sind ihr Hauptziel. Zwar sind alle anderen Datenquellen ebenso verfügbar, aber die Quellen-TKÜ soll diese nur verwenden, um das Bestehen einer Telekommunikationsverbindung abschätzen zu können und dann die Aufnahme zu starten.[156]

Verbundene WLANs/Mobilzellen Wann das infiltrierte informationstechnische System mit welchem drahtlosen Netzwerk verbunden war, ist genauso ersichtlich, wie die Zugangsdaten der verschiedenen Netzwerke.

GPS Signale Dass jedes angeschlossene Gerät ausgelesen werden kann, sorgt auch dafür, dass bei vorhandenem GPS-Empfänger und GPS-Empfang jederzeit die Standortdaten abgefragt und gespeichert werden können.

Ein- und Ausschaltvorgänge des Systems Die Informationen, wann ein System ein- oder ausgeschaltet wurde, sind genauso verfügbar für die ODS wie die Möglichkeit, das System ein- bzw. auszuschalten.

Diese Aufzählung soll beispielhaft veranschaulichen, welche Möglichkeiten sich der ODS bieten. Sie ist nicht vollständig und kann es auch nicht sein, da die ODS vom infiltrierten System aus jegliche angeschlossene Geräte abfragen und steuern kann.

[156] Chaos Computer Club, *QUELLEN-TKÜ-Stellungnahme des Chaos Computer Clubs*, 2009.

3.1.7 Speicherung und Übermittlung der Funde

Die von der ODS durch den oben beschriebenen Suchvorgang als relevant erachteten Daten müssen bis Abgriff oder Übermittlung auf dem System des Betroffenen vorgehalten werden,[157] weil nicht davon ausgegangen werden kann, dass immer zur Zeit der Datensuche genug Netzwerkdurchsatz zur Verfügung steht. Es muss daher auf den Speichermedien des Systems selbst weiterer Platz belegt werden, indem die ODS Daten im Zielsystem platziert.[158] Eine Speicherung einfacher Verweise auf gefundene Daten wird im Allgemeinen nicht genügen, da so dem Löschen und Verändern der Daten durch den Benutzer nicht begegnet werden kann.

Auch die gespeicherten Daten müssen versteckt werden, damit sie nicht von normalen benutzergesteuerten Dateisuch- und Indizierungsprogrammen gefunden und indiziert werden. Die ODS bewerkstelligt dies durch Verschlüsseln und Ablegen der Daten in freien Speicherbereichen des Systems.[159] So entsteht ein Bereich auf dem System des Betroffenen, den nur die ODS kontrolliert.

Für die Übermittlung der Funde gibt es generell zwei Möglichkeiten: Entweder wird auf die Datenträger des infiltrierten Systems physisch direkt zugegriffen (z. B. bei einer Grenzkontrolle, Hausdurchsuchung), oder aber die Daten werden über das Internet zu den infiltrierenden Behörden übermittelt. Dabei muss unterschieden werden, ob die ODS aktiv die Verbindung zu den Behördenrechnern sucht oder auf dem System Möglichkeiten schafft, von außen kontaktiert zu werden. Durch die zunehmende Nutzung von Internetzugängen durch Router mit Firewalls und Network Address Translation (NAT) sind private Systeme jedoch immer seltener direkt mit dem Internet verbunden, also auch nicht direkt von „außen“ ansprechbar.[160] Für mobile Endgeräte gelten die gleichen Kontaktschwierigkeiten, denn die Internetprovider verwenden in dieser Domäne fast ausschließlich NAT-Adressen. Beim Internet Protokoll Version 6 (IPv6), dem Nachfolger der aktuell verwendeten Version 4 (IPv4) ist die Nutzung von NAT zwar nicht mehr nötig, doch dafür ist die Dynamisierung von Adressen zum Zwecke der Zielverschleierung für Dritte explizit vorgesehen.[161]

Hinzu kommt: Von außen ansprechbare Software stellt immer auch ein Sicherheitsrisiko für das System dar — besonders wenn sie hinter dem Rücken des Betroffenen betrieben wird. Daher ist sinnvollerweise angedacht „dass die Software weder von außen erkannt noch angesprochen werden kann“.[162]

Die Rücksendeadresse, an welche die Funde im Falle einer Übermittlung versendet werden sollen, kann entweder direkt als IP-Adresse oder als vollqualifizierter Domänenname (FQDN-Notation) gespeichert sein. Darüber hinaus muss unterschieden werden, ob die Rücksendeadresse in einer eigenen Konfigurationsdatei gespeichert oder direkt in den Quellcode der ODS geschrieben und somit in den Binärcode hineinkompiliert wird.

---

[157] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort auf Frage 39.

[158] Ganz im Gegenteil zur Behauptung A.a.O. Antwort auf Frage 25.

[159] A.a.O. Antwort auf Frage 36c.

[160] Chaos Computer Club, *QUELLEN-TKÜ-Stellungnahme des Chaos Computer Clubs*, 2009, Seite 15 ff.

[161] RFC (Request for Comments) 4941: Privacy Extensions for Stateless Address Autoconfiguration in IPv6.

[162] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort auf Frage 6.

Da speziell sichergestellt werden soll, „dass die Software nicht ohne erheblichen Aufwand dazu veranlasst werden kann, an einen anderen Server als den von den Sicherheitsbehörden benutzten Server zurückzumelden“,[163] kommt nur die direkte Quellkodierung der Rücksende-IP-Adresse in Frage. Diese Lösung ist weniger flexibel, aber auch weniger anfällig für externe Faktoren.
Die Übermittlung der Funde muss über sichere, verschlüsselte Kanäle erfolgen,[164] da sie sehr wahrscheinlich personenbezogene private Daten, belastende Daten oder beides enthalten werden. Bis zur Kenntnisnahme durch einen Menschen in der ausforschenden Stelle ist generell nicht klar, was für Daten tatsächlich übertragen werden.
Welcher Weg der Übermittlung im Endeffekt gegangen wird, hängt von vielen Faktoren wie erwarteter Zeit, die das System online sein wird, erwartetem Netzwerkdurchsatz, erwarteter Fundgröße oder erwarteter Auffälligkeit der Übermittlung ab.[165]
Für die Verschlüsselung der Funde[166] auf dem lokalen System sowie deren Übermittlung sind symmetrische und asymmetrische Verfahren denkbar. Bei der symmetrischen Verschlüsselung nutzen Sender und Empfänger den gleichen Schlüssel; eine Signierung von Nachrichten ist somit nicht möglich, weil notwendigerweise nicht nur der Sender den Schlüssel besitzt.[167] Für asymmetrische Verfahren benötigt jeder Kommunikationspartner ein Schlüsselpaar, bestehend aus einem geheimen privaten Schlüssel und einem öffentlichen Schlüssel. Daten, die mit dem einen Schlüssel verschlüsselt werden, sind mathematisch bedingt nur mit dem jeweils anderen Schlüssel (ohne übermäßig hohen Aufwand) entschlüsselbar.[168]
Versand: Für den verschlüsselten Datenversand bildet der sendende Telekommunikationspartner eine „Hash“ genannte Prüfsumme über die Daten und verschlüsselt diese mit seinem privaten Schlüssel. Diesen Hash fügt er nun an die Daten und verschlüsselt beides mit dem öffentlichen Schlüssel des Empfängers. Dadurch kann später nur der Empfänger mit seinem privaten Schlüssel das Empfangene entschlüsseln.
Empfang: Der Empfänger der Daten verwendet nun seinen privaten Schlüssel, um die Daten und den verschlüsselten Hash zu erhalten. Mit dem öffentlichen Schlüssel des Absenders kann nun der Hash entschlüsselt und mit einem frisch über die Nachricht erzeugten Hash verglichen werden. Stimmen diese überein, kann die Nachricht nur vom Besitzer des (zum öffentlichen Schlüssel des Absenders gehörenden) privaten Schlüssels erzeugt worden sein.
Ein verlässlicher Betrieb asymmetrischer Verfahren inklusive Signierung ist folglich nur dann gewährleistet, wenn private Schlüssel ausschließlich beim Besitzer vorliegen.[169]

Für die ODS bietet sich eine asymmetrische Verschlüsselung mit dem öffentlichen Schlüssel der ausforschenden Behörde an, so dass auch bei Bekanntwerden von ODS-Schlüsseln oder der Funde die schon verschlüsselten Daten geschützt bleiben. Dennoch muss erwähnt werden,

[163] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort zu Frage 6.
[164] A.a.O. Antwort zu Frage 28.
[165] Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seite 5.
[166] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort auf Frage 39.
[167] Anderson, *Security Engineering*, 2008, Seite 147 ff.
[168] A.a.O. Seite 170 ff.
[169] A.a.O. Seite 147 ff.

dass bei korrekter Anwendung des asymmetrischen Paradigmas die schon verschlüsselten Daten zwar nur von der ODS-erstellenden Stelle entschlüsselt werden können, die Signierung aber nicht verlässlich sein kann, da die ODS (inklusive ihrem privatem Schlüssel) auf einem fremden System arbeitet und diesem zur Verfügung steht. Zu den direkten technischen Folgen siehe Abschnitt 3.3 (Fehlende Protokollierbarkeit).

Die Übermittlung der Funde kann einmal, mehrmals oder auch kontinuierlich erfolgen. Der Umstand, dass die ODS während der Übertragung mit der ausführenden Stelle in Verbindung steht, kann auch für eine Aktualisierung der Suchkriterien, Update der Software und sonstige Neuausrichtung der Maßnahme genutzt werden.

3.1.8 Deaktivierung / Entfernung vom Zielsystem

Sobald die Maßnahme beendet (abgeschlossen oder abgebrochen) wird, müssen die ODS und etwaige Funde wieder vom informationstechnischen System des Betroffenen entfernt werden.[170] Dazu gibt es mehrere Möglichkeiten:

Die ODS könnte so konstruiert werden, dass sie sich auf ein während der Übermittlung der Funde gesendetes Löschsignal hin selbständig deaktiviert und löscht.[171] Weil aber nicht sicher ist, wann oder ob das System des Beobachteten das nächste Mal eine Verbindung zum Internet aufbaut — also mit der ODS kommuniziert werden kann, stellt das eine unsichere Lösung dar. Eine vom Internet unabhängige Lösung besteht in der Implementierung eines zeitgesteuerten Mechanismus, so dass sich die ODS nach einer gewissen Aktivitätsdauer selbsttätig deaktiviert bzw. vom System des Betroffenen löscht[172] oder dies generell nach einer bestimmten Zeit ohne Internetverbindung tut.[173] „Als Zeitgeber werden außer der Systemzeit weitere Zeitberechungsmodule parallel eingesetzt“,[174] damit die „Selbstdeinstallation der ODS auch nach einem evt. Wiederaufsetzen des Systems mittels Back-Up initiiert“[175] wird.

Ist der Deaktivierungs- und Löschungsgrund der ODS im Abbruch des Ermittlungsverfahrens gegen den Betroffenen zu finden, muss die Software unverzüglich abschaltbar sein. Dies kollidiert konzeptionell mit der Anforderung, „dass die Software weder von außen erkannt noch angesprochen werden kann.“[176] Hier muss eine Entscheidung getroffen werden.

Die sicherste Methode ist wieder die händische Deinstallation vor Ort am System, wobei sie nur technisch einfach umzusetzen ist, der physische Zugriff (Wohnung, Büro etc.) muss anderweitig organisiert werden. Letztendlich sollen die am System vorgenommenen Änderungen durch die Deinstallationsroutinen rückgängig gemacht werden.[177]

---

[170] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort zu Frage 30.

[171] Krasemann und Ziercke, *Interview u. a. zur Online-Durchsuchung*, 2007, 2:57 Minuten.

[172] A.a.O. 2:59 Minuten.

[173] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort auf Frage 18.

[174] A.a.O. Antwort auf Frage 22.

[175] A.a.O. Antwort auf Frage 30.

[176] A.a.O. Antwort auf Frage 6.

[177] A.a.O. Antwort auf Frage 40.

3.2 Die Unterscheidung von Quellen-TKÜ und Online-Durchsuchung

Nach der obigen Analyse des Lebenszyklus kann nun die politisch behauptete Unterscheidung der technischen Umsetzung von Online-Durchsuchung und Quellen-TKÜ[178] betrachtet werden. Alle Schritte, von der Einbringung ins Zielsystem bis hin zur Deaktivierung, werden von den Maßnahmen technisch auf die gleiche Weise realisiert. Die einzige Unterscheidung ist die Auswahl der Hauptdatenquellen, siehe Unterabschnitt 3.1.6 (Datensuche). Die exakte Wahl ist sehr wichtig, denn die Unterscheidung Quellen-TKÜ / Online-Durchsuchung wird mit einer strengen Limitierung der Quellen-TKÜ auf Telekommunikationsdaten und der Online-Durchsuchung auf alle anderen Datenarten begründet.[179]

Zunächst zur Quellen-TKÜ: Die Quellen-TKÜ-Software liest hauptsächlich jene Datenquellen aus, die vermutlich zur Telekommunikation genutzt werden sollen. Wenn die Software einen laufenden Telekommunikationsvorgang detektiert, werden sie ausgelesen und die erhaltenen Daten ausgeleitet.[180] Da jedoch nur anhand zusätzlicher Informationen und Daten des infiltrierten informationstechnischen Systems[181] überhaupt versucht werden kann zu detektieren, ob gerade ein Telekommunikationsvorgang stattfindet und welche Datenquellen (Audio/Video/E-Mail/etc.) Teil dieses Vorgangs sind, ist die behauptete strenge Suchbeschränkung, „ausschließlich [...] Daten, die Gegenstand der Telekommunikation sind,“[182] zu analysieren, technisch nicht haltbar und zusätzlich im Nachhinein nicht belegbar.[183] Schlägt die Detektierung (Start/Ende und Datenarten der Telekommunikation) fehl, werden in der Folge Daten ausgeleitet, die nicht Teil eines Telekommunikationsvorgangs sind. Darüber hinaus muss eine Quellen-TKÜ-Software auch Daten im System platzieren können: Um den ausforschenden Stellen auch offline vorbereitete und verschlüsselt zu übertragende Kommunikationsdaten (Z. B. die Nutzung eines Mailclients mit Verschlüsselungsfunktion im Offline-Modus) zuleiten zu können, müssen diese Daten durch die Quellen-TKÜ-Software offline abgefangen und dann auf dem System zwischengelagert werden, bis eine Übermittlung möglich wird; z. B. wenn das System online geht oder die Datenträger abgeholt werden.

Eine Quellen-TKÜ ist also mit den geforderten Fähigkeiten unter Beachtung der behaupteten Limitierungen technisch nicht realisierbar.

Auch umgekehrt ist eine Unterscheidung der beiden Instrumente zwar politisch gewollt,[184] aber technisch äußerst fragwürdig: Jede Online-Durchsuchung hat potenziell Zugriff auf alle

[178] Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Vorbemerkung.
[179] Bundesregierung der 16. Wahlperiode, *Drucksache 16/6535*, 28.9.2007, Antwort auf Frage 14.
[180] Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seiten 8 und 9 vergleiche auch Chaos Computer Club, *QUELLEN-TKÜ-Stellungnahme des Chaos Computer Clubs*, 2009, Seite 18.
[181] Siehe z. B. Abschnitt 3.1.6 (Ein- und ausgehender Netzwerkverkehr) oder Abschnitt 3.1.6 (Aktuell laufende Prozesse/installierte Programme).
[182] Bundesregierung der 16. Wahlperiode, *Drucksache 16/6535*, 28.9.2007, Antwort auf Frage 14.
[183] Siehe Abschnitt 3.3 (Fehlende Protokollierbarkeit).
[184] Siehe Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seite 7.

Datenquellen, darunter Telekommunikationsdaten[185] sowie die dazugehörigen Verbindungsdaten. Die angedachte Beschränkung der Suche auf Daten, die nicht Teil eines Telekommunikationsvorganges sind, unterliegt jedoch den gleichen Abgrenzungsproblemen, wie sie die Quellen-TKÜ hat. Werden z. B. von der Online-Durchsuchungs-Software Bildschirmfotos angefertigt, ist es nicht auszuschließen, dass der Betroffene gerade seinen Bildschirminhalt via Bildschirmübertragungssoftware mit anderen teilt, eine durchsuchte E-Mail soeben empfangen wurde oder eine analysierte Datei gleich verschickt wird,[186] ganz zu schweigen von zugreifbaren anfallenden Verkehrsdaten.[187] Eine verlässliche Beschränkung auf Nicht-Kommunikationsdaten ist auch hier weder möglich noch im Nachhinein belegbar.[188]

Technisch sind die beiden Instrumente folglich identisch, und wenn die „inhaltliche Abgrenzung zur Quellen-TKÜ" darin besteht, dass die Online-Durchsuchung „sich nicht auf Telekommunikationsdaten erstreck[en](t)"[189] und umgekehrt, muss man zu dem Schluss kommen, dass die beiden Instrumente auch inhaltlich praktisch nicht zu unterscheiden sind. ODS und QTKÜS sind daher von der Wirkung auf den Betroffenen identisch. Anders ausgedrückt: *Beide Maßnahmen, sowohl Online-Durchsuchung als auch Quellen-TKÜ, werden mit der ODS realisiert.*

Eine tiefergehende Analyse der Unterscheidung Telekommunikationsdaten/Nicht-Telekommunikationsdaten ist weiter unten im Unterabschnitt 4.1.1 (Wohnraumüberwachung, Telekommunikationsüberwachung, Quellen-TKÜ und die Online-Durchsuchung) zu finden.

Verfassungsrechtlich zum gleichen Schluss kommen Ulf Buermeyer (Richter des Landes Berlin und derzeit an die Senatsverwaltung für Justiz abgeordnet) und Prof. Dr. Matthias Bäcker (Juniorprofessor für Öffentliches Recht an der Universität Mannheim).[190]

3.3 Fehlerszenarien der ODS

Entlang des Lebenszyklus der ODS existieren viele Fehlerszenarien. Zwar werden an dieser Stelle triviale Implementationsfehler nicht betrachtet,[191] doch bei allen diesbezüglichen Überlegungen muss im Hinterkopf behalten werden, dass es den Umständen geschuldet keine ausführliche Testphase einer ODS vor dem Einsatz geben kann. Dabei wäre es für Software mit diesen Anforderungen und diesem Komplexitätsgrad nach den Regeln guter Softwareentwicklung notwendig. In einem Satz: „Fehlerfreiheit ist nicht zu erwarten."[192]

[185] Siehe z. B. Abschnitt 3.1.6 (Ein- und ausgehender Netzwerkverkehr), Abschnitt 3.1.6 (Kamera- und Mikrofondaten) und Abschnitt 3.1.6 (Aktuell laufende Prozesse/installierte Programme).

[186] Vergleiche Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seite 2.

[187] Siehe Sieber, *Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen*, 9.10.2007, Seite 3.

[188] Siehe Abschnitt 3.3 (Fehlende Protokollierbarkeit).

[189] Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seite 7.

[190] Buermeyer und Bäcker, „Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO", 2009.

[191] Obwohl sie wahrscheinlich sind, siehe „0zapftis" Chaos Computer Club, *Report 23*, 8.10.2011 und Chaos Computer Club, *Report 42*, 26.10.2011.

[192] Bogk (Chaos Computer Club), *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007, Seite 16.

Im folgenden Abschnitt werden einige der Szenarien analysiert, die als prinzipiell nicht oder nur teilweise beherrschbar angesehen werden müssen.[193] Für einen Rechtsstaat ist eine technische Risikoanalyse unumgänglich, weil nur so Überlegungen zur Möglichkeit angemessener Nutzung eines derartig eingriffstiefen Instruments anzustellen sind: „Bei der Entwicklung werden besonders die Aspekte [...] des weitestgehenden Ausschlusses unerwünschter Effekte berücksichtigt".[194] Folgende unerwünschte Szenarien sind denkbar und möglich:

Weiterverbreitung Bei „der Entwicklung werden besonders die Aspekte [...] der Nichtweiterverbreitung von hierzu verwendeten Programmen [...] berücksichtigt".[195] Eine Weiterverbreitung vom infiltrierten System aus kann technisch verhältnismäßig einfach verhindert werden, da diese Funktionalität — im Gegensatz z. B. zum Verändern/Anlegen von Daten — nicht mit anderen gewünschten Fähigkeiten der ODS kollidiert. Allerdings ist eine Verbreitung möglich, indem initial viele Systeme unbeabsichtigt infiltriert werden. Diese wäre keine Weiterverbreitung im klassischen Sinne, wie etwa durch Würmer, dennoch wären potenziell viele Systeme betroffen. Dazu mehr im nächsten Punkt.

Falsches System infiltriert Die verschiedenen Einbringungsmethoden haben unterschiedliche Treffgenauigkeiten bezüglich des zu infizierenden Systems. Soll z. B. einem Benutzer via präparierter E-Mail, Webseite oder CD/USB-Stick eine ODS untergeschoben werden, kann es sein, dass er sie von einem anderen als seinem eigenen Rechner aus öffnet, z. B. bei Freunden, im Internetcafé oder im Büro am geschäftlich genutzten Firmencomputer. Ein Weiterleiten der kompromittierenden, aus Sicht des Betroffenen harmlosen Nachrichten/Weblinks ist genauso ohne weiteres denkbar, wie das versehentliche Platzieren derartiger Dateien in Peer-to-peer-Netzwerken. Im schlimmsten Fall würde die ODS installiert und ihrem Programm folgend Daten suchen, um sie an die untersuchende Behörde zu übermitteln. All das kann unter Umständen viele Betroffene erzeugen.
Auch bei der Ausnutzung von Sicherheitslücken für die entfernte Installation der ODS kann es, wie in Unterabschnitt 3.1.3 (Einbringung ins Zielsystem / Infiltration) beschrieben, zu Problemen kommen, da die Erkennung des Zielsystems aus Sicht der ODS nicht trivial ist. Insbesondere wenn es über seine IP-Adresse im Internet identifiziert und angegriffen werden soll, denn der größte Teil privater Internetanschlüsse bekommt bei jeder Anmeldung beim Internetprovider eine dynamische IP-Adresse zugewiesen. Beim Trennen dieser Internetverbindung wird die verwendete Adresse wieder frei und vom Provider für einen anderen Anschluss erneut verwendet.[196] Noch komplexer wird das Zielproblem dadurch, dass sich viele Computer hinter Firewalls oder NAT-Routern befinden.[197] Dabei teilen sich mehrere netzwerkfähige Geräte eine Internetadresse und treten nur über vom lokalen Router dynamisch vergebene Ports mit anderen Internetrechnern in Verbindung. Dadurch sind sie von anderen Computern, die sich auch im gesicherten Netz befinden, nicht ohne weiteres unterscheidbar. So kann es passieren, dass Ports, die gerade für einen Rechner geöffnet worden sind, schon kurze Zeit später für

[193] Vergleiche Pfitzmann, *Skript zu den Vorlesungen Datensicherheit und Kryptographie*, 1990-2000, Seite 11.
[194] Bundesregierung der 16. Wahlperiode, *Drucksache 16/4997*, 10.4.2007, Antwort zu Frage 4.
[195] A.a.O. Antwort zu Frage 4.
[196] Chaos Computer Club, *QUELLEN-TKÜ-Stellungnahme des Chaos Computer Clubs*, 2009, Seite 15 ff.
[197] A.a.O. Seite 15 ff.

einen anderen verwendet werden. Gleiches gilt in hohem Maße für Endgeräte, die über das Mobilfunknetz ins Internet gehen.

Um vor der Infiltration eines erreichten Systems sicherzustellen, dass es sich um das Zielsystem handelt, müsste die ODS es zunächst untersuchen oder durchsuchen können. Dies ist offensichtlich nicht möglich, weder bei der Online-Durchsuchung noch bei der Quellen-TKÜ. Dieses Problem kann nur durch die direkte Installation vor Ort umgangen werden.

Finden von (für den Investigationsgrund) irrelevanten Daten Zusätzlich zum Senden von Daten unbeteiligter Personen bzw. derer Systeme ist es sehr wahrscheinlich, dass die Suchkriterien so weit gefasst werden, dass auch Daten ins Ergebnisraster fallen, die wenig bis nichts mit dem Investigationsgrund zu tun haben, worunter auch Daten höchstpersönlichen und privaten Inhalts fallen. Andererseits sollen die relevanten Daten auch nicht ausgefiltert werden, man denke nur an „handschriftliche" Notizen mit Stift auf einem Tabletcomputer, die technisch kein Text-, sondern ein grafisches Format hätten. Dies ist kein rein technisches Problem und wird daher erst in Unterabschnitt 4.1.4 (Technischer Kernbereichsschutz) behandelt und erklärt werden.

Übermitteln der Funde an die falsche Stelle In Abhängigkeit von der Implementation der Zieladresse im Übermittlungsmodul (IP-Adresse oder als vollqualifizierter Domänenname, Konfigurationsdatei oder Quellcode) kann es auf verschiedene Weise passieren, dass die Funde nicht an die intendierte Stelle gesendet werden. Im wahrscheinlichen Falle der Speicherung der IP-Adresse im Quellcode der ODS würde nur ein Zahlendreher bei der Beauftragung der ODS die Zusendung missglücken lassen. Routingfehler des Internets werden der Seltenheit wegen hier nicht betrachtet.

Für den Fall, dass die Daten nicht an die intendierte Adresse übermittelt werden, kann und muss kryptographisch abgesichert werden, dass sie für den Empfänger unbrauchbar sind.

Veränderung von Daten auf dem System Abgesehen von der grundsätzlichen Änderung der Daten des Systems durch die Aufbringung der ODS selbst verändert sie strenggenommen allein beim Suchen kontinuierlich die durchsuchten Daten.[198] Darüber hinaus werden durch das Speichern der Funde auf dem System[199] notwendigerweise *neue Dateien angelegt*. Doch auch andere Daten sind potenziell betroffen. Durch unvorhergesehene „Interaktionen" mit auf dem System vorhandenen Programmen (z. B. Antivirenprogrammen oder Viren/Würmern/Trojanern) oder Unachtsamkeit bei der Programmierung der ODS[200] kann es zu Erstellung, Veränderung oder Löschung von Daten kommen. Diese Möglichkeit umfasst durch die Privilegierung der ODS potenziell alle Daten des Systems sowie die von dort aus zugreifbaren Netzspeicher. Diese Gefahr könnte durch eine zuverlässige Protokollierung abgefangen werden.

[198] Siehe Unterabschnitt 3.1.6 (Datensuche).
[199] Siehe Unterabschnitt 3.1.7 (Speicherung und Übermittlung der Funde).
[200] Siehe Chaos Computer Club, *Report 23*, 8.10.2011, Seite 1 ff.

Fehlende Protokollierbarkeit

Eine „systemtechnische Protokollierung aller Zugriffe und Aufspielungen auf den betroffenen Rechner“[201] vom Behördensystem aus greift zu kurz, weil die Aktivitäten der ODS auf dem betreffenden Rechner nicht eingeschlossen werden können. Trotz vorhandener technischer Verfahren zur Sicherstellung der Authentizität von Daten[202] sind deren notwendige Voraussetzungen — exklusive Kontrolle über das System — in diesem Fall nicht gegeben, da die ODS sich auf einem fremdkontrollierten System befindet.[203] Durch die Infiltration haben beide Systeme ihre Integrität verloren; das Zielsystem, weil ein fremdes Programm auf Systemebene operiert, und die ODS, weil ihre Daten dem fremden System gänzlich zugreifbar und veränderbar vorliegen.

Konkret bedeutet dies, dass signierte Logdateien nicht vertrauenswürdig sind, weil die nötigen privaten Schlüssel der ODS auf dem System selbst liegen müssen, also auch dem fremden System vollends zur Verfügung stehen. Bei Einsatz von symmetrischer Verschlüsselung wäre nicht einmal der Versuch einer Authentifizierung oder Signierung möglich. Es ist folglich falsch, dass „technisch [...] durch verschiedene Funktionalitäten, wie etwa [...] (durch den) Einsatz von Hash- und/oder Verschlüsselungsverfahren oder digitaler Signatur die Integrität der übertragenen Daten überprüfbar gemacht werden“ kann.[204] *Protokolle einer ODS können ihre Aktivität auf dem fremden System nicht belegen*, denn so gesehen ist auch für die ODS an sich die Vertraulichkeit und Integrität dort nicht gewährleistbar. „Gefährliche“ Funktionen wie etwa Schreibrechte auf Nutzerdaten können auch nicht grundsätzlich deaktiviert werden, ohne dass die ODS dadurch komplett unbrauchbar würde, siehe Unterabschnitt 3.1.4 (Verankerung im System).

Selbst wenn die ausführende Stelle die Software zur Gänze verstehen würde und z. B. bei Gericht der Quellcode der ODS präsentiert werden könnte,[205], wären die konkreten Aktivitäten der ODS nicht rekonstruierbar, weil sie ununterbrochen mit einem komplexen System — dem infiltrierten Wirt — interagieren muss, dessen Zustände schon während der Maßnahme unbekannt waren und es somit um so mehr im Nachhinein sind. Die Belegkette müsste natürlich auch alle im Nachhinein eingespielten Updates und Modifikationen umfassen, was die Komplexität einer tatsächlichen Ablaufanalyse ins Unendliche steigert. *Die Aktivitäten der ODS auf dem infiltrierten System sind folglich auch im Nachhinein nicht rekonstruierbar.* Selbst nach einer — praktisch unmöglichen, aber hier rein hypothetisch angenommenen — erfolgreichen Bewältigung dieses Problems stünde der Beleg immer noch aus, dass auch wirklich das Kompilat des vorgelegten Quellcodes verwendet wurde, „schließlich könnte dafür eine andere als die hinter-

[201] Ziercke, *Sprechzettel für die Teilnahme des Präsidenten des Bundeskriminalamtes Jörg Ziercke an der 53. Sitzung des Innenausschusses zu TOP 24a (24b, 24c)*, 19.10.2011, Seite 2.

[202] Anderson, *Security Engineering*, 2008, Seite 147 ff.

[203] Hansen und Krause, *Heimliche Online-Durchsuchung – Wie geht's, wie schütze ich mich?*, 2007, Seite 30.

[204] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort zu Frage 3.

[205] Das war eigentlich angedacht (siehe A.a.O. Frage 26) jedoch sagte BKA-Präsident Jörg Ziercke am 19.10.11 im Innenausschuss des Bundestages: „Richtig ist, dass der Quellcode der Quellen-TKÜ-Software der Firma Digitask dem BKA nicht offen gelegt wurde. Auch die Quellcodes anderer kommerzieller Anbieter wurden dem BKA nicht offen gelegt.“ Ziercke, *Sprechzettel für die Teilnahme des Präsidenten des Bundeskriminalamtes Jörg Ziercke an der 53. Sitzung des Innenausschusses zu TOP 24a (24b, 24c)*, 19.10.2011, Seite 12.

legte Software-Version eingesetzt [...] worden sein".[206] Komplexerer Angriffe z. B. gegen den Compiler der ODS sind zwar möglich,[207] werden jedoch hier nicht weiter betrachtet. Die Auswirkungen dieser technischen Umstände auf die Aussagekraft der erhaltenen Daten werden weiter unten in Unterabschnitt 4.2.4 (Aussagekraft von Daten mit extrinsischer Personenbeziehbarkeit) behandelt.

Da die Veränderung von Daten auf dem System notwendige Voraussetzung, aber auch notwendige Konsequenz für den Einsatz der ODS sind, kann sie gleichzeitig bei den gewollten und ungewollten Funktionen der ODS genannt werden.

Ungewollte Veröffentlichung des ODS-Binär- oder -Quellcodes Es ist möglich, dass der Binär- oder sogar Quellcode der ODS bekannt wird. Dies kann u. a. durch eine unvollständige Löschung der ODS vom System eines Betroffenen und anschließender Rekonstruktion, durch zwangsweise Offenlegung bei Gericht[208] oder durch unzufriedene Behördenmitarbeiter mit Affinität zum Wistleblowing geschehen. In diesem Fall würden nicht nur Antiviren- und andere Sicherheitssoftwarehersteller ihre Programme sofort so anpassen, dass sie die ODS aufspüren können, sondern eventuell verwendete Sicherheitslücken und die zugehörigen Exploits kämen in Umlauf. Das würde jedes dem ursprünglichen Zielsystem der ODS ähnliche System gefährden. Im schlimmsten Fall wären z. B. alle Windowsversionen betroffen.[209] Aber das sind nicht alle Folgen, auch geöffnete Ports und eventuelle Fehler der ODS an sich würden öffentlich bekannt und ausnutzbar.
Für die infiltrierenden Behörden hätte die Offenlegung noch weitere große Nachteile, denn die Rücksendeadressen für ODS-Funde würden zwangsläufig mitveröffentlicht werden. Das würde erstens das Blocken von Netzverkehr zu diesen Adressen möglich machen, zweitens würden bei einem Wechsel der Adressen die Funde von noch operierenden ODS für die Dauer der Operation an falsche Rücksendeadressen übermittelt werden, und drittens könnte nun auch das Behördensystem Ziel vielfältiger Angriffe werden.

Schaffung von Sicherheitslücken durch die ODS Jedes zusätzliche Programm in einem System erhöht dessen Komplexität. Insbesondere wenn das Programm im Kernelmode läuft und sich in vorhandene Abläufe einklinkt, sind die Folgen von Fehlern oder unvorhergesehenen Programmkonstellationen nicht absehbar.[210] Wenn die Eingriffe der ODS sich nicht nur auf das Durchsuchen von Dateien, Mitspeichern von Tastenanschlägen oder Anfertigen von Screenshots beschränkt, sondern auch der Netzverkehr belauscht, Hardwareeinstellungen modifiziert, Firewallkonfigurationen geändert und sogar Ports geöffnet werden, ist die Fehleranfälligkeit sehr hoch, besonders weil sich die Software nicht ausgiebig in Feldtests behaupten

[206] Siehe Fox, *Stellungnahme zur „Online-Durchsuchung", Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, 29.9.2007, Seite 13 und Bogk (Chaos Computer Club), *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007, Seite 16.
[207] Thompson, „Reflections on Trusting Trust", Aug. 1984.
[208] Krasemann und Ziercke, *Interview u. a. zur Online-Durchsuchung*, 2007, 3:07 Minuten.
[209] Siehe die Windows-LNK-Lücke, Schmidt, *Microsoft bestätigt USB-Trojaner-Lücke*, 17.7.2010.
[210] Einige Computersicherheitsexperten halten Personal Firewalls und Virenscanner für unnötige Komplexitätsvergrößerer, siehe z. B. Bernauer und Wiechers, *Personal Firewalls versagen*, 13.12.2004.

oder als fehlerhaft herausstellen konnte. Dies kann ernsthafte Sicherheitsrisiken für das System des Betroffenen bedeuten. Wie und von wem diese ausgenutzt werden könnten, ist nicht abschätzbar.

Unmöglichkeit der Deaktivierung / Entfernung vom Zielsystem Aus den in Unterabschnitt 3.1.8 (Deaktivierung / Entfernung vom Zielsystem) diskutierten Möglichkeiten zur Deaktivierung und Löschung der ODS kann mögliches Fehlverhalten abgeleitet werden. Die drei wichtigen Szenarien sind erstens, wenn das infiltrierte System sich unerwartet nicht mehr mit dem Internet verbindet, die Löschung jedoch per entferntem Kommando erfolgen sollte, zweitens wenn die zeitgesteuerte Deaktivierung und Deinstallation fehlschlägt und drittens, wenn Spuren oder Bestandteile der ODS im System verbleiben, weil die Deinstallationsroutine nicht alle Änderungen zurücksetzen konnte. In den beiden ersten Fällen bleibt die ODS über den intendierten Zeitraum hinaus aktiv, im dritten Fall entstehen Entdeckungsrisiko und eventuell später unvorhersehbare Wechselwirkungen mit dem System. Letztgenannter Fall ist wahrscheinlich.[211]

Verletzung der Verfügbarkeit eines Systems Ein extremer Fall der Einflussnahme der ODS auf das Zielsystem läge vor, wenn das Zielsystem durch die Aktivitäten der ODS funktionsunfähig werden würde. Dieser Umstand kann viele Ursachen haben, hauptsächlich aber die Veränderung von essentiellen Konfigurations- oder Treiberdateien, sei es durch eine fehlerhafte Veränderung des Bootablaufs bei dem Versuch, sich als Bootkit[212] zu installieren,[213] die Störung von Eingabegeräten bei dem Versuch, einen Softwarekeylogger zu verankern und zu aktivieren oder ganz trivial beim fehlerhaften Einlesen und Durchsuchen von Dokumenten, deren Dokumentenstandards proprietär sind. Dabei kann es zu Fehlern kommen, die das System beeinträchtigen und im schlimmsten Fall auch zum Absturz bringen können.[214]

Verletzung der Vertraulichkeit und Integrität eines Systems Die gewünschten Funktionen der ODS sind, wie aus Unterabschnitt 3.1.4 (Verankerung im System) folgt, ausschließlich unter Verletzung von Vertraulichkeit und Integrität des Zielsystems realisierbar. Dies hat seine prinzipiell-konzeptionellen Ursachen im Charakter der Maßnahme („heimliches Eindringen“) und ist kein Fehler der modernen Computersystemarchitektur; wie etwa eine heimliche Hausdurchsuchung nicht ohne das Öffnen der Schlösser, das Betreten der Räume und Durchsuchen der Sachen durchgeführt werden kann. Da die Verletzung der Vertraulichkeit und Integrität des Systems notwendige Konsequenz, aber auch notwendige Voraussetzung für den Einsatz der ODS sind, muss sie gleichzeitig bei den gewollten (Investigation) und ungewollten (übermäßiger Eingriff in Grundrechte) Eigenschaften der ODS genannt werden.

---

[211] Freiling, *Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, 27.9.2007, Seite 7.

[212] Tanenbaum, *Modern operating systems*, 2008, Seite 677.

[213] Das Stoned-Bootkit kann „auch für Ermittlungsbehörden interessant sein, etwa zur Entwicklung eines Bundestrojaners“. Ries und Backfeld, *Bootkit hebelt Festplattenverschlüsselung aus*, 30.7.2009 oder noch tiefer, der BIOS-Trojaner Eikenberg, *Die Rückkehr des BIOS-Trojaners*, 12.9.2011.

[214] Bogk (Chaos Computer Club), *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007, Seite 18.

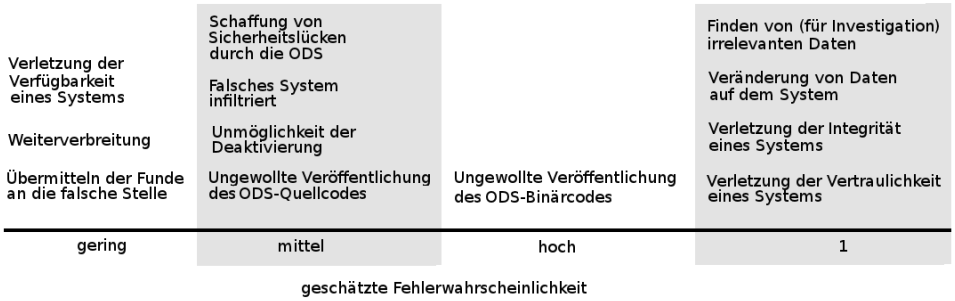


Abbildung 3: Abschätzung der Fehlerszenarien (ohne Abstrahlungsanalyse)

3.4 Zusammenfassung der Analyse der Funktionen

Zusammenfassend kann festgehalten werden, dass die ODS tief in das zu infiltrierende System eingreifen und dort umfassende Kontrollmöglichkeiten erlangen muss, um effektiv und effizient heimlich darauf suchen und insgesamt agieren zu können. Die Informationssuche selbst kann bei klassischen, textbasierten Dokumenten anhand syntaktischer Kriterien realisiert werden, bei vielen Datenquellen müssen aber alle Daten aufgehoben werden, da eine Auswertung (noch) nicht automatisiert erfolgen kann. Die gesammelten Daten werden auf dem System vorgehalten und wenn möglich zur entsprechenden Stelle übermittelt oder vor Ort abgeholt. Da die ODS auf einem fremden System operiert, sind keine ihrer Aktivitäten verlässlich belegbar oder rekonstruierbar. Darüber hinaus ist eine Unterscheidung in Online-Durchsuchung und Quellen-TKÜ technisch nicht nachvollziehbar. Abschließend wurde eine Abschätzung möglicher Fehlerszenarien vorgenommen, einige davon werden regelmäßig eintreten.
Im obigen Abschnitt wurden zu erwartende technische Probleme einer solchen Maßnahme angesprochen; die weniger technischen, sondern eher konzeptionellen und gesellschaftlichen Folgen und Probleme werden nun diskutiert.

4 Technisch-konzeptionelle und gesellschaftliche Folgen der Online-Durchsuchung

Im vorherigen Kapitel wurden die Eigenschaften einer ODS für die Online-Durchsuchung auf technisch-konzeptioneller Ebene analysiert und diskutiert, doch informationstechnische Systeme und deren Software, inklusive der ODS, operieren nicht im luftleeren Raum oder in gänzlich formalisierter Umgebung, sondern im menschlichen Kontext mit komplexer Wechselwirkung. Sie sind durch die Modellierung technischer und sozialer Prozesse mit formalen Mitteln zwar im Kern technisch, aber durch ihren Einsatz in gesellschaftlich-sozialer Interaktion auch „sozial wirksam“.[215] Besondere Beachtung verdient dabei, dass die informatische Modellierung dieser Prozesse durch die Struktur und Grenzen der Mittel Handlungslogiken erzeugen, die kein Ergebnis offen geführter gesellschaftlicher Diskurse sind, sondern unreflektiert als scheinbar

[215] Siehe Coy, „Brauchen wir eine Theorie der Informatik?“, 1989, Seite 17.

natürlich übernommen werden.[216] Dies gilt um so mehr, je weiter sich informationstechnische Systeme von wirtschaftlichen Arbeitsinstrumenten hin zu alltäglichen Unterhaltungsmedien, privaten Kommunikationszentralen, allgegenwärtigen Begleitern[217] und sogar zum digitalen Rückzugs-„Ort“ entwickeln. Insbesondere, wenn der Einsatz von informationstechnischen Mitteln tief in das Leben von Menschen eingreift und es sofort oder später möglicherweise maßgeblich beeinflusst, noch dazu ohne ihr Mitwirken oder Mitwissen, ist eine kritische Betrachtung dieser informationstechnischen Mittel, der Motivation ihres Einsatzes und der intendierten und tatsächlichen Effekte notwendig. Dies gilt für den privatwirtschaftlichen Einsatz wie z. B. Scoring oder Online-Banking genauso wie für die Durchführung hoheitlicher Aufgaben, was den Kontext dieser Arbeit darstellt.

Somit musste die Fragestellung nach den Folgen einer Online-Durchsuchung zunächst eine technische Perspektive einnehmen, die die Konsistenz von Anforderungen, technische Seiteneffekte oder technische Fehlerszenarien analysiert. Sie muss aber notwendigerweise auch den darüber hinausgehenden gesellschaftlichen Aspekt mit einbeziehen. Dieser muss die Einordnung der Funktionen und Eigenschaften einer solchen Software in den gesellschaftlich-sozialen und rechtlichen Kontext beinhalten und dann technisch-konzeptionell bedingte Vorgaben und theoretisch-informationstechnische Grenzen dorthin übertragen, um auf derartig verursachte Probleme und Folgen hinzuweisen. Entscheidend dabei ist, dass diese Probleme und Folgen nicht lediglich als zufällige Phänomene beschrieben und verstanden werden, sondern explizit als Konsequenz einer informationstechnischen Herangehensweise.[218]

4.1 Einordnung und Auswirkungen der technischen Möglichkeiten der Software

Ein wichtiger Teil der Rechte der Bürger in Deutschland sind Abwehrrechte — Abwehrrechte des Individuums gegenüber einem übermächtigen Staat.[219] Diese Rechte sorgen dafür, dass der Bürger nicht nur darauf zu vertrauen braucht, dass ihm eine wohlwollende Exekutive ein würdevolles Leben ermöglicht, sondern dass er ein Recht darauf hat und es bei Verletzung desselben grundsätzlich auch einklagen kann.[220] Konsequenz dieses individuenzentrierten Staatsverständnisses ist es, dem Staat für die Erledigung seiner Aufgaben prinzipiell nicht alle erdenklichen, auch grundrechteeinschränkende Handlungsoptionen zuzugestehen, aus denen er dann nach Gutdünken einige auswählt und von anderen absieht, sondern ihm von vornherein für bestimmte Aufgaben maximal bestimmte Möglichkeiten an die Hand zu geben und ihm andere, stärker rechteeinschränkende Möglichkeiten auch zu verwehren; nicht im Sinne einer Absichtserklärung, sondern effektiv und sanktioniert zu verwehren. Die Beschränkung des für die Erledigung einer Aufgabe Erlaubten darf demnach nicht davon abhängig sein, ob die Möglichkeiten tatsächlich genutzt werden würden oder nicht.

[216] Vergleiche Coy, „Brauchen wir eine Theorie der Informatik?“, 1989, Seite 25.

[217] Siehe z. B. Apple Inc. *Learn more about Siri*, 2011.

[218] Die Probleme des Einsatzes von Wahlcomputern sind ein exemplarischer Fall dieser informationstechnischen Konsequenzen, siehe 46halbe, *Chaos Computer Club: HSG Wahlsysteme bestätigt Unzulänglichkeit ihrer Wahlcomputer*, 16.10.2006.

[219] Artikel 1-20 GG, siehe Pieroth und Schlink, *Grundrechte*, 2010, Seite 21 ff.

[220] Siehe die Aufgaben des Bundesverfassungsgerichts bei A.a.O. Seite 306 ff.

Dieses Verständnis muss sich auch in den Werkzeugen des Staates wiederfinden: für bestimmte Zwecke und Aufgaben erlaubte Mittel dürfen auch nur maximal den Zweck erfüllende Funktionen haben, wenn von diesen Funktionen Gefahren für Grundrechtsträger ausgehen. Polizeibeamten bestimmter Aufgabenbereiche sind daher beispielsweise Handfeuerwaffen gestattet, aber keine Sturmgewehre oder gar die beliebige Verwendung von physikalisch-chemischen Maschinen jedweder Art.[221]

Für die Beurteilung und verfassungsrechtliche Abwägung von Grundrechtseingriffen für bestimmte Zwecke ist das *Verhältnismäßigkeitsprinzip* allgemein anerkannt.[222] Dabei wird überprüft, ob die grundrechteeinschränkende Maßnahme legitim, geeignet, erforderlich und angemessen ist. Eine Maßnahme ist legitim, wenn ihr Zweck grundsätzlich im Bereich der dem Staate übertragenen Aufgaben liegt. Geeignet ist eine Maßnahme, wenn sie dem Zweck grundsätzlich kausal dienen kann. Erforderlich ist sie, wenn kein schwächeres Mittel geeignet ist, diesem Zweck zu dienen. Angemessen — oder verhältnismäßig im engeren Sinne — ist eine Maßnahme, wenn die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht.[223] An dieser Stelle muss eine Rechtsgüterabwägung erfolgen, die der Gesetzgeber grundsätzlich schon in der Ermächtigung vorgeben muss.
Genügt eine Maßnahme dem Verhältnismäßigkeitsprinzip, so gilt sie als verfassungskonform. Vom Staat eingesetzte informationstechnische Mittel müssen natürlich auch unter diesem Gesichtspunkt überprüft werden.[224]
In Bezug auf die Online-Durchsuchung ist es demnach nötig, nicht nur die Funktionen und Eigenschaften, die zur Erreichung des Einsatzzweckes notwendig sind, zu betrachten, sondern auch die darüber hinausgehenden, nicht intendierten oder unterschlagenen grundrechteeinschränkenden Möglichkeiten und Funktionen der eingesetzten Software.

An dieser Stelle seien also die Funktionen, Möglichkeiten und Eigenschaften der Online–Durchsuchung noch einmal zusammengefasst:
Die Online-Durchsuchung muss auf dem infiltrierten System mindestens mit den Rechten des Betroffenen laufen, um seine Daten nach relevanten Inhalten durchsuchen zu können, kann also auch mit dessen Benutzerkonto jegliche Daten erstellen, verändern oder löschen,[225] beliebige Programme starten,[226] verbundene Geräte abfragen und steuern. Aktivitäten und Begrenzungen der Software können einer dritten Stelle (z. B. dem Gericht) nicht technisch begründbar glaubhaft gemacht werden. Funktionalitäten sind durch Kontaktaufnahme mit der ODS und Einspielung/Installation von Updates beliebig nachladbar, veränderbar und auch wieder deaktivierbar.

[221] Pfitzmann, *Rede vor dem Bundesverfassungsgericht als Sachverständiger zur Online-Durchsuchung*, 10.10.2007, Seite 1.
[222] Pieroth und Schlink, *Grundrechte*, 2010, Seite 66 ff.
[223] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 227.
[224] A.a.O. Absatz 218.
[225] Siehe Abschnitt 3.1.4 (Lese- und Schreibrechte für Nutzerdaten, Usermode) vergleiche auch diesbezügliche Vorhaben: Krempl und Ziegler, *Bayerischer Landtag setzt den "Bayerntrojaner"frei*, 3.7.2008.
[226] Z. B. Audio- bzw. Videoaufnahmeprogramme Bogk (Chaos Computer Club), *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007, Seite 15.

Um das Entdeckungsrisiko auf dem fremden System gering zu halten und auf erweiterte Systemdaten (z. B. Hauptspeicher auslesen, Tastatureingaben mitlesen) zuzugreifen, muss die Software im privilegierten Kernelmode laufen.
Abgesehen von naheliegendem Zubehör informationstechnischer Systeme wie etwa Kameras, Mikrofone, externe Festplatten, Drucker, Tastatur, Maus oder Netzwerkgeräte sind natürlich auch eventuell vorhandene GPS-Empfänger, Beschleunigungssensoren, Neigungssensoren oder Chipkartenleser ansprechbar. Letzteres ist gerade in Verbindung mit dem neuen Personalausweis oder chipkartenbasiertem Online-Banking interessant. Die Geräte für eine audiovisuelle Komplettüberwachung sind somit, wenn vorhanden, einsatzbereit und werden sogar vom Betroffenen selbst gewartet. Ist das infiltrierte System ein mobiles Endgerät, kann zudem davon ausgegangen werden, dass es sich bei den Standortdaten des Gerätes um den Aufenthaltsort des Betroffenen handelt.
Mit den erweiterten Rechten des Kernelmodus kann die ODS auch Netzwerkverkehr nicht nur speichern oder ausleiten, sondern ausgehenden Verkehr z. B. komplett umleiten und verändern, so dass die Netzwerkverkehrsanalyse oder die komplette Imititation eines Netzwerkpartners auf leistungsfähigere externe Systeme ausgelagert werden kann.
Immer verbreiteter werden auch computergestützte Heimüberwachungssysteme mit mehreren steuerbaren Kameras und Mikrofonen für Innen und Außen. Diese werden genauso kontrollierbar durch die ODS wie computergesteuerte Babyfone oder Hausklimaanlagen.

4.1.1 Wohnraumüberwachung, Telekommunikationsüberwachung, Quellen-TKÜ und die Online-Durchsuchung

Die technische Gleichheit von Online-Durchsuchung und Quellen-TKÜ wurde bereits in Unterabschnitt 3.2 (Die Unterscheidung von Quellen-TKÜ und Online-Durchsuchung) gezeigt, dennoch reicht die Gleichheit viel weiter und führt zu tieferliegenden, grundsätzlichen Problemen.
Die Quellen-TKÜ ist eine Maßnahme, die dem Zweck der Telekommunikationsüberwachung (TKÜ) von Personen dienen soll. Sie soll dann eingesetzt werden, wenn die Zielpersonen sich durch die Verwendung digitaler, verschlüsselter Kommunikationskanäle einer Überwachung an Infrastrukturpunkten entziehen. Sie hat die Aufgabe, Kommunikationsdaten „am Endgerät (der „Quelle“) noch vor der Verschlüsselung bzw. nach ihrer Entschlüsselung“[227] abzufangen und den Überwachenden zuzuführen. So möchte man der Kommunikationsdaten habhaft werden, auch wenn sie während der eigentlichen Kommunikation nicht sinnvoll auswertbar vorliegen.
Dabei ist die Quellen-TKÜ softwaretechnisch eine Online-Durchsuchung, deren „Leistungsumfang [...] beschränkt“[228] sein soll. Wie in Unterabschnitt 3.2 (Die Unterscheidung von Quellen-TKÜ und Online-Durchsuchung) erläutert, ist die Beschränkung, ja sogar die Beschränkungsmöglichkeit zwar prinzipiell anzuzweifeln, aber das Konzept „Quellen-TKÜ“ soll hier unter einem anderen Aspekt analysiert werden.

[227] Ziercke, *Sprechzettel für die Teilnahme des Präsidenten des Bundeskriminalamtes Jörg Ziercke an der 53. Sitzung des Innenausschusses zu TOP 24a (24b, 24c)*, 19.10.2011, Seite 4.
[228] A.a.O. Seite 4.

Die Befürworter argumentieren, dass „nur die Daten im Rahmen eines laufenden Telekommunikationsvorgangs überwacht werden, die für die Versendung in das Kommunikationsnetz vorgesehen sind. Durch eine Quellen-TKÜ werden also keine Daten erlangt, die nicht auch durch eine „konventionelle“ TKÜ – außer dem Umstand der Kryptierung – erlangt werden können“.[229]

Allerdings ist die Frage, welche Daten überhaupt für die Versendung vorgesehen sind, schwer technisch zu beantworten, denn grundsätzlich weiß das nur der Versender selbst. Den Daten ist es nicht anzusehen. Dass dies keine rein akademisch-theoretische Frage ist, zeigt der eingangs erwähnte Beschluss des Landgerichts Landshut vom 20.1.2011, der das Verständnis der Behörden, eine E-Mail im Entwurfsstadium sei für die Versendung vorgesehen, korrigierte und die betreffende Maßnahme für rechtswidrig erklärte. Die Unklarheit ging sogar so weit, dass sich der amtierende Bundesinnen- und Verfassungsminister Friedrich zu folgender Aussage hinreißen ließ:

> Das Landgericht Landshut sagt, es sei nicht erlaubt. Die bayerische Staatsregierung sagt, es sei erlaubt. Man kann ja auch anderer Auffassung sein als ein Landgericht.[230]

Was die Unterscheidung, welche Daten für die Versendung vorgesehen sind und welche nicht, so folgenschwer macht, sind die Auswirkungen einer falschen Entscheidung. So wird aus einer Quellentelekommunikationsüberwachung eines Videochats (z. B. mit der Software Skype) schnell eine audiovisuelle Wohnraumüberwachung, wenn die Zielperson den Stummschalteknopf der Software aktiviert.[231] Dann nehmen die angeschlossene Kamera und das Mikrofon — somit auch die Quellen-TKÜ — weiterhin das Geschehen auf, aber die Software verschlüsselt und verschickt nur ein schwarzes Bild und Stille. Zu erkennen, wann tatsächlich telekommuniziert wird und welche Datenarten übertragen werden, ist technisch sehr schwer und mitnichten zufriedenstellend gelöst,[232] weil die zu überwachende Software (in diesem Fall die Videochatsoftware) nicht automatisch mit der Quellen-TKÜ zusammenarbeitet. Hier muss versucht werden, aus anderen Systemdaten Anhaltspunkte abzuleiten oder direkt in die zu überwachende Kommunikationssoftware einzugreifen. Im Falle des Eingreifens stünden dann jedoch eine Vielzahl von über die aktuelle Telekommunikation hinausgehenden Daten zur Verfügung (z. B. sämtliche Verbindungsdaten oder aufgezeichnete Kommunikationsdaten), was explizit untersagt wurde.[233]

Für annehmbare Ergebnisse müssten die Audio- und Videodaten dauerhaft auf „Telekommunikationsverhalten“ des Betroffenen hin ausgewertet werden, für die in beiden Fällen (Versuch der Detektion und personelle Überwachung) stattfindende audiovisuelle Wohnraumüberwachung gelten jedoch aus gutem Grund ganz andere rechtliche Hürden.[234]

---

[229] A.a.O. Seite 4.

[230] Hoffmann und Tomik, *„Es gibt keine rechtliche Grauzone“*, 15.10.2011.

[231] Chaos Computer Club, *QUELLEN-TKÜ-Stellungnahme des Chaos Computer Clubs*, 2009, Seite 4.

[232] A.a.O. Seite 4 und 14.

[233] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 190.

[234] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum großen Lauschangriff*, 3.3.2004, Leitsatz 4.

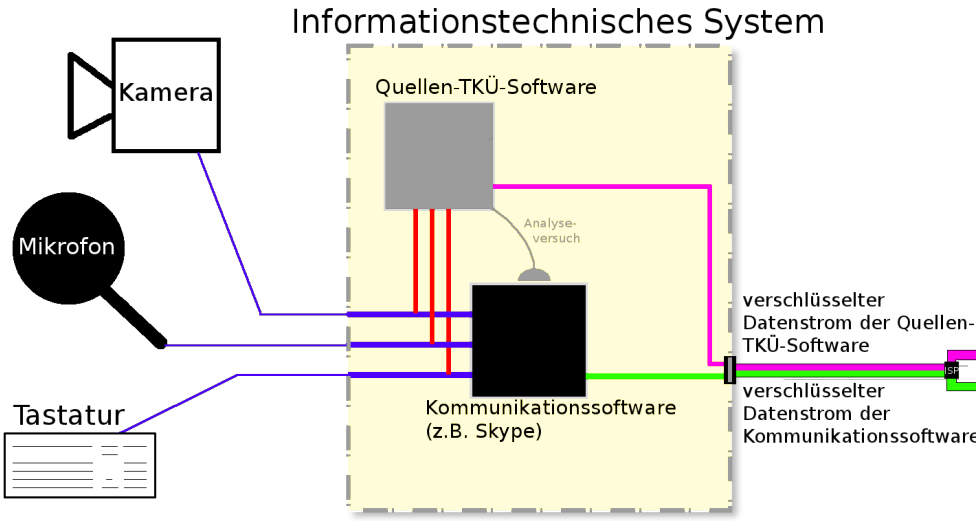


Abbildung 4: Funktionsschema einer Quellen-TKÜ (Beispiel: Audio/Video/Tastatur): Der Abgriff findet vor dem Versenden statt

Die Möglichkeit einer audiovisuelle Wohnraumüberwachung ist nicht einmal bei der Online-Durchsuchung angedacht,[235] dennoch ist sie für eine Quellen-TKÜ trotz ihres „beschränkten Leistungsumfanges“ einfach so möglich. Dies zeigt, wie ähnlich sich diese Maßnahmen nicht nur technisch, sondern auch konzeptionell sind.

Auch der zweite Teil der obigen Aussage, es „werden [...] keine Daten erlangt, die nicht auch durch eine „konventionelle“ TKÜ [...] erlangt werden können“, wird durch das gegebene Beispiel ad absurdum geführt. Klarer wird dies durch ein Gedankenexperiment: Angenommen, die Quellen-TKÜ hätte ein Orakelmodul, das ihr korrekt signalisiert, wann welcher Datenstrom Gegenstand eines Telekommunikationsvorganges ist. Folglich würde die Quellen-TKÜ immer zur richtigen Zeit die richtige Datenquelle anzapfen und ausleiten können. Die Crux an der Sache ist jedoch, dass Videotelefoniesoftware wie Skype die zu übertragenden Daten vor dem Versand je nach Internetverbindung standardmäßig mehr oder weniger stark komprimiert, was zu hohen Detailverlusten der Daten führen kann. Während sich der Telekommunikationspartner auf der anderen Seite in einem Beispielszenario möglicherweise mit mäßiger Telefonqualität zufrieden geben muss, greift die Quellen-TKÜ das qualitativ hochwertige Originalsignal an der Datenquelle ab.[236] Ob die ausforschende Stelle in diesem Beispiel einem Hund im Hintergrund oder dem Gespräch am Nebentisch Beachtung schenkt, ist zweitrangig, denn dass der Telekommunikationspartner diese Informationen gar nicht bekommt, weil sie „wegkomprimiert“

[235] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort auf Frage 23 und Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seite 7.

[236] Vergleiche Chaos Computer Club, *QUELLEN-TKÜ-Stellungnahme des Chaos Computer Clubs*, 2009, Seite 18.

worden sind, ist die eigentliche Erkenntnis des Gedankenexperiments. Dabei geht es nicht darum, welche Details exakt verloren gehen, sondern darum, dass sich die mit der Quellen-TKÜ gewonnenen Daten von den Daten der Telekommunikation grundsätzlich unterscheiden. Die Aussage, es wäre „programmtechnisch sichergestellt, dass die Ausleitung der Audiodaten nur während eines Skype-Telefongesprächs erfolgt“,[237] ist folglich nicht nur technisch falsch, sie zeigt auch gänzliches Unverständnis des problematischen Sachverhalts.

Die Ursache der beiden Probleme — Versendungsabsicht und Datenunterschied — ist in der Ursache der „Notwendigkeit“ einer Quellen-TKÜ begründet. Gemäß ihrem intendierten Zweck soll sie Daten vor der ausgehenden Verschlüsselung abfangen, sofern sie zur Versendung vorgesehen sind. Wenn sie aber zur Versendung vorgesehen sind, steht die Versendung in das Kommunikationsnetz noch bevor; die Daten sind also noch keine Telekommunikationsdaten. Genau deshalb wird die Quellen-TKÜ gefordert, eben weil die eigentlichen Telekommunikationsdaten wertlos sind.

Eine Quellen-TKÜ-Maßnahme geht also davon aus, dass bestimmte Daten auf einem infiltrierten informationstechnischen System bald Telekommunikationsdaten sein werden, und fängt sie einfach vorher ab, um sie — als vermeintliche Telekommunikationsdaten — auszuleiten. Selbst wenn man die implizite Erweiterung des Begriffes „Telekommunikationsdaten“ auf Daten, die zur Versendung vorgesehen sind, mitträgt, ist die Unterscheidung in Nichttelekommunikationsdaten und Bald-Telekommunikationsdaten prinzipiell-technisch nicht sicher realisierbar. Problematische Fälle sind nicht nur E-Mailentwürfe, offline geschriebene Mails, die noch verschickt werden müssen,[238] E-Maildateianhänge oder Webcamdaten, sondern darunter fallen auch spezielle Ordner, deren Dateien ununterbrochen synchronisiert — also versendet — werden, und Tastenanschläge in Chat- und Sofortnachrichtenprogrammen oder Online-Kollaborationswerkzeugen[239] fallen darunter.[240]

Es müssten Annahmen darüber gemacht werden, in welchen technischen Zuständen des infiltrierten Systems man davon ausgehen könnte, dass gerade ein Telekommunikationsvorgang mit welchen Datenquellen stattfindet, um dann das System auf vielfältige Hinweise darauf zu überwachen. Wegen dieser Systemüberwachungsnotwendigkeit und der oben beschriebenen prinzipiellen Probleme kann eine Beschränkung der Quellen-TKÜ „auf Daten aus einem laufenden Telekommunikationsvorgang [...] durch technische Vorkehrungen“[241] prinzipiell weder sichergestellt noch belegt werden,[242] sie muss also immer mindestens als vollwertige Online-Durchsuchung angesehen werden.[243]

[237] Bundesregierung der 16. Wahlperiode, *Drucksache 16/6885*, 30.10.2007, Seite 3.
[238] Vergleiche Bogk (Chaos Computer Club), *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007, Seite 3.
[239] Siehe z. B. die Webanwendung *Etherpad*.
[240] Vergleiche Fox, *Stellungnahme zur „Online-Durchsuchung“, Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, 29.9.2007, Seite 16.
[241] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 190.
[242] Siehe Abschnitt 3.3 (Fehlende Protokollierbarkeit).
[243] Bäcker, „Das IT-Grundrecht“, 2009, Seite 21.

Kritik der Ausweitung des Telekommunikationsdatenbegriffs

So man die implizite Erweiterung des Begriffes „Telekommunikationsdaten“ auf zur Versendung vorgesehene Daten jedoch nicht mitträgt, stellt sich die Frage, ob eine Quellen-TKÜ aus einem infiltrierten „Quell“system heraus überhaupt zulässig sein kann. Oder anders gefragt, gibt es *innerhalb* eines informationstechnischen Systems einer Person überhaupt Telekommunikationsdaten laufender Telekommunikationsvorgänge? Es ist die Frage, wo genau im informationstechnischen Kontext der Übergang von gespeicherten Daten zu Telekommunikationsdaten schlüssig gesetzt werden kann. Wäre die Grenze eines informationstechnischen Systems die Stelle, ab welcher zu verschickende Daten zu Telekommunikationsdaten werden, dann könnte eine Quellen-TKÜ niemals Telekommunikationsdaten abfangen, weil sie selbst nur im System agieren kann.

Andererseits könnte man behaupten, dass die Versendung schon dann beginnt, wenn vom Benutzer systeminterne Prozesse derart angestoßen worden sind, dass in Kürze von einer automatischen Versendung ausgegangen werden kann, doch diese Vorverlagerung — es ist noch nichts versendet worden — würde nicht der Idee des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) entsprechen. Dieses schützt, wie das Bundesverfassungsgericht in einem Urteil begründet, den Telekommunikationsvorgang: „Der spezielle Schutz des Fernmeldegeheimnisses durch Art. 10 GG schafft einen Ausgleich für den technisch bedingten Verlust an Beherrschbarkeit der Privatsphäre, der durch die Nutzung von Anlagen Dritter zwangsläufig entsteht“,[244] denn „der Nutzer kann sich bei den seiner Verfügungsmacht unterliegenden Geräten gegen den unerwünschten Zugriff Dritter durch vielfältige Maßnahmen schützen“.[245] Im zitierten Fall waren die fraglichen Daten durch das Recht auf informationelle Selbstbestimmung und gegebenenfalls durch die Unverletzlichkeit der Wohnung geschützt.[246] Kern des Fernmeldegeheimnisses ist also die fehlende Kontrolle über kommunizierte Inhalte, während sie „unterwegs“ sind, sich also nicht im „Herrschaftsbereich eines Kommunikationsteilnehmers (befinden), wo dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann.“[247]

Eine technische verkürzte Sicht auf den Sachverhalt könnte die Grenze direkt in das physikalische Netzwerkinterface des eigenen Computers legen, denn erst dort endet die Möglichkeit, eigene Schutzvorkehrungen treffen zu können. Am Interface außen anliegende Daten, ob eingehend oder ausgehend, wären Kommunikationsdaten; innen anliegende Daten nicht, da ihre Kontrolle nur vom Wissensstand des Systembesitzers, nicht aber vom Wohlwollen Dritter abhinge.

Doch, so das Bundesverfassungsgericht in einem anderen Urteil, „die Reichweite des Schutzes des Fernmeldegeheimnisses endet nicht am sogenannten Endgerät der Telekommunikationsanlage. Dem Schutzanliegen des Art. 10 Abs. 1 GG wird eine solche rein technisch definierte Abgrenzung angesichts der technologischen Entwicklungen und insbesondere der durch sie bedingten vielfältigen Konvergenzen der Übertragungswege, Dienste und Endgeräte nicht ge-

[244] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zu Verbindungsdaten*, 2.3.2006, Absatz 81.
[245] A.a.O. Absatz 79.
[246] A.a.O. Erster Leitsatz.
[247] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 185.

recht".[248] Diese Beschreibung bezieht sowohl dem Kommunikationspartner unbekannte Mithörfunktionalität, als auch „eine Vielzahl von Leistungen (mit ein), auch solche, die untrennbar in den Übermittlungsvorgang eingebunden und dem Endteilnehmer häufig gar nicht in den Einzelheiten bekannt sind". Das Fernmeldegeheimnis schützt somit nicht (nur) die Daten der laufenden Telekommunikation, sondern deren Inhalt. Daher reicht es in andere Schutzbereiche hinein.
Es wäre ein seltsamer rechtsstaatlicher Zug, TKÜ-Maßnahmen, die zur Erlangung von Telekommunikationsdaten einen Eingriff in das Fernmeldegeheimnis erlauben, für das Eindringen in andere Schutzbereiche zu missbrauchen. Dies könnte mit gutem Grund als *rechtliches* Trojanisches Pferd bezeichnet werden, dessen Unzulässigkeit gewiss ist.

Trägt man die implizite Erweiterung des Begriffes „Telekommunikationsdaten" auf zur Versendung vorgesehene Daten also nicht mit, kann eine Quellen-TKÜ aus einem infiltrierten System heraus ausschließlich Daten erlangen, die sich im Schutzbereich mehrerer anderer Grundrechte befinden. Eine Ermächtigung für den Eingriff ins Fernmeldegeheimnis genügt daher nicht.

4.1.2 Metapherkritik einer „digitalen Hausdurchsuchung"

Im Online-Durchsuchungsdiskurs wurde oft die *Hausdurchsuchung* als Metapher verwendet, um Suchweise, Eingriffstiefe und Qualität der gefundenen Daten zu illustrieren.[249] Metaphern sind zwar praktisch, um eine ganz grundsätzliche Vorstellung von unbekannten oder abstrakten Dingen zu bekommen, aber ihre Funktionsweise basiert auf einer Begriffssystemübertragung von einem bekannten auf einen neuen Bereich.[250] Je nach Metapher stößt man früher oder später an deren Grenze, ohne es aber zu merken, denn das Neuland ist ja unbekannt. Ab dieser Tiefe des Übertragens von Begriffen und Begriffsbeziehungen in den neuen Bereich kann es von lehrreich-interessant[251] bis hin zu fatal falsch werden. Die Metapher der Hausdurchsuchung für eine Online-Durchsuchung ist so ein Fall, bei dem es schnell fatal falsch werden kann.

Wie eingangs beschrieben, ist eine Durchsuchung eine „im Grundsatz auf Offenheit angelegte Maßnahme",[252] aber auch, wenn man von einer *geheimen Hausdurchsuchung* sprechen würde, bliebe die Hausmetapher. Sie ist sinnvoll, wenn es darum geht, den Denkfokus auf die Privatsphäre des Individuums und seine unverletzliche Wohnung zu richten, aber sie impliziert auch, dass der Betroffenen das, was durchsucht wird, grundsätzlich kennt und kontrolliert; dass dort nichts ist, was er nicht dort hingebracht hat, dass er die grundsätzliche Struktur versteht und erklären kann. Jeder Bürger kennt und „begreift" seine Wohnung, aber die wenigsten kennen

[248] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum Mithören an Telekommunikationseinrichtungen*, 9.10.2002, Achter Leitsatz.
[249] Siehe z. B. Bundesregierung der 16. Wahlperiode, *Drucksache 16/4997*, 10.4.2007, Antwort zu Frage 17 oder Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort zu Frage 2.
[250] Vergleiche Goodman, *Languages of Art*, 1976, Seite 81 ff.
[251] Vergleiche A.a.O. Seite 74 ff.
[252] Bundesgerichtshof, *Kein heimlicher Zugriff auf ein Computersystem zum Zwecke der Strafverfolgung*, 25.11.2006, Absatz 4.

und begreifen ihr informationstechnisches System.[253] Zum einen liegt das an der Komplexität moderner Computersysteme und zum anderen an der Dynamik solcher Systeme. Die Kombination sorgt dafür, dass nicht einmal Experten ihr System gänzlich verstehen können.[254] Es ist eben nicht einfach nur da und lässt sich verwenden, sondern „tut" selbst Dinge im Hintergrund und ist hochgradig rückgekoppelt. Es sucht WLANs, lädt Updates, lässt sich mit Viren infizieren, sammelt Positionsdaten, weist auf Netzwerkangriffe hin, hilft anderen Rechnern im Netzwerk, verschluckt Dateien, blockiert Verbindungen, indiziert Mails, macht Selbsttests, stürzt ab, versendet Spam, verschlagwortet Fotos, speichert Webseiten und führt auch sonst viele Operationen aus, die der Benutzer nicht explizit angestoßen hat. Eine Wohnung dagegen ist passiv, statisch, räumlich begrenzt und zur Gänze sinnlich wahrnehmbar, was dafür sorgt, dass sie mühelos „verstanden" werden kann.

Das gilt für Computersysteme nicht. Viele Menschen wollen sie nicht einmal verstehen und sind froh, wenn sie einfach funktionieren. Das Interessante daran ist aber, dass sich das Leben und Miteinander der Menschen immer mehr in die digitale Sphäre verschiebt, und zwar schneller, als Menschen lernen, mit ihrem Computer richtig umzugehen oder zu wissen, was sich alles darauf befindet und abspielt. Somit sammelt sich immer mehr digitales Ich aus E-Mails, Texten, Fotos, Chatlogs, Browser-Lesezeichen, Passwörtern, Bankdaten, Arbeitsdokumenten, Fernsehshows, Notizen, Musikstücken und deren jeweiligen Nutzungsdaten an einem einzigen Ort an,[255] ohne dass dieser vom analogen Ich kognitiv durchdrungen wird. Begünstigt wird diese Entwicklung neben der allumfassenden Vernetzung dadurch, dass es in einer digitalen Umgebung einfacher ist, Daten aufzuheben als sie zu löschen,[256] bzw. es mehr Gründe gibt, sie aufzuheben als sie zu löschen. Eine neue (Online)-Festplatte ist einfacher beschafft, als die digitale Sphäre in Ordnung zu halten und nicht mehr Benötigtes an die Müllabfuhr zu übergeben, so wie man es vielleicht mit einer Wohnung machen würde, wenn es irgendwann eng wird. Vor Freude über die fehlende räumliche Beschränkung und die vernetzten digitalen Möglichkeiten darf jedoch die Akkumulation von Persönlichem in unverstandener Form nicht unreflektiert bleiben. All diese Aspekte werden von einer Hausdurchsuchungsmetapher ignoriert und erzeugen den Eindruck einer grundsätzlichen Beherrschbarkeit der Maßnahme. Sowohl von der durchsuchenden als auch der durchsuchten Seite ist dies größtenteils nicht gegeben.

Eine Grundeigenschaft der digitalen Welt ist die kontinuierliche Generierung von Datenspuren durch die Verwendung informationstechnischer Systeme durch den Einzelnen. Anders als in der analogen Welt wird im digitalen Raum mit Werkzeugen gearbeitet, die ihre Aktivitäten und deren Umstände speichern und archivieren. Dies ist nicht notwendigerweise so, ist aber sehr einfach möglich und zudem praktisch: Erstens zur Fehlererkennung einzelner Softwarefunk-

[253] Schneier, *Secrets and Lies*, 2004, Seite 6-7.
[254] A.a.O. Seite 6 ff.
[255] Siehe A.a.O. Seite 33 oder Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 171.
[256] Vergleiche Meyer-Schönberger, *Nützliches Vergessen*, 2008.

tionen,[257], zweitens zur Angriffserkennung und -abwehr und für die Systemanalyse,[258] drittens weil es teilweise gesetzlich verlangt wird[259] und viertens zur Erhöhung des Nutzerkomforts.[260] Die Browserhistorie ist vielen Benutzern noch ein Begriff, aber alles darüber Hinausgehende wird vielleicht unbewusst genutzt, aber nicht im eigentlichen Sinne wahrgenommen.[261] Langsam findet eine Sensibilisierung der Nutzer und Hersteller statt,[262] jedoch langsamer, als der dunkle Datenberg wächst.

Diese Entwicklung schafft zusammen mit dem Fortschritt in Technologie und Rechenleistung ein für das Individuum nur mit großem Aufwand beherrschbares Zentrum höchstpersönlicher Informationen, die erstens dem Benutzer zu einem Teil nicht bekannt sind und zweitens eine zeitliche Dimension beinhalten, die dem Nutzer größtenteils verborgen bleibt. Dieses immer größer werdende digitale Gravitationszentrum der Persönlichkeit eines Menschen ist das Ziel der heimlichen Online-Durchsuchung. So ist es nicht von prophetischem Charakter, dass ein Sachverständiger bei der mündlichen Anhörung des Bundesverfassungsgerichtes zur Online-Durchsuchung Folgendes äußerte:

> Gegeben die technische Entwicklung, wird Freiheit und Unbeobachtbarkeit des Denkens (etwa beim Erwägen von Äußerungen oder Handlungen) künftig untrennbar mit dem Schutz persönlichster Rechner, ihrer Anwendung und auch der Daten auf ihnen verknüpft sein. [...] Der Zugriff auf gespeicherte Computerdaten auf persönlichsten Rechnern entgegen des Willens des Eigennutzers ist daher künftig weniger mit einer klassischen Hausdurchsuchung vergleichbar, als vielmehr mit der Verabreichung bewusstseinsverändernder Drogen zum Zwecke des Erlangens von Aussagen.[263]

Wenn man also unbedingt die Hausdurchsuchungsmetapher anwenden wollte, müsste man eher davon sprechen, dass unbekannte Beamte heimlich dauerhaft mit in die Wohnung einzögen, alle Räume, Schränke, Wände, Böden und Decken durchsuchten und teilweise umbauen würden, alles sehen, hören, riechen und befühlen, ja sogar begrenzt Gedanken lesen und in die Vergangenheit schauen könnten. Der letzte Teil wird im Folgenden näher ausgeführt.

4.1.3 Kern der Sache: Schattendaten und ihre zeitliche Permanenz

Die Online-Durchsuchung profitiert in hohem Maße davon, dass Benutzer ihr System nicht verstehen. Wie oben kurz angedeutet, scheinen aber auch die Befürworter dieser Maßnahme deren

[257] Anderson, *Security Engineering*, 2008, Seite 192 ff.
[258] A.a.O. Seite 660 ff.
[259] Z. B. das damalige Gesetz zur Vorratsdatenspeicherung TKG §113a und b.
[260] Für ein Komplettlogging des Nutzerverhaltens zu diesem Zwecke siehe das Zeitgeist-Projekt, Huber, *GNOME Zeitgeist – Eine neue Art des Findens*, 5.7.2009.
[261] Der Wirkkreis der Person ist damit größer als ihr Merkkreis, vergleiche dazu Wiegerling u. a., „Ubiquitärer Computer – Singulärer Mensch“, 2008, Seite 75. Eine Betrachtung dieser Eigenschaft informationstechnischer Systeme würde jedoch an dieser Stelle zu weit führen.
[262] Vergleiche Bogk (Chaos Computer Club), *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007, Seite 3.
[263] Pfitzmann, *Rede vor dem Bundesverfassungsgericht als Sachverständiger zur Online-Durchsuchung*, 10.10.2007, Seiten 3 und 4.

Möglichkeiten in einem informationstechnischen System nicht hinreichend gut zu verstehen. So schrieb das Bundesinnenministerium zu einer Frage zu Funden der Online-Durchsuchung: „Sofern in der Frage als Beispiel das Tagebuch angeführt wird, ist es für die Grundrechtsposition des Betroffenen im Übrigen irrelevant, ob das Tagebuch im Rahmen einer offenen Durchsuchung/Sicherstellung/Beschlagnahme, unter Umständen an einem versteckten Ort, aufgefunden und gesichtet oder in elektronischer Form qua Online-Durchsuchung durch die Polizei festgestellt wird.“ [264] Hier wird offensichtlich verkannt, dass dem genannten Tagebuch in digitaler Form — anders als in der materiellen Welt — viele Metadaten anhaften. Gleiches gilt für jegliche Funde, daher hat folgende Erklärung exemplarischen Charakter.

Der Fund des digitale Tagebuchs würde nicht nur die eigentlichen Inhalte zutage fördern, sondern je nach System auch, wann es das letzte Mal gelesen wurde, wann verändert, wo gespeichert, möglicherweise sogar welche Änderungen vorgenommen wurden. Natürlich ist es auch eingebettet in die digitale Landschaft des Systems, wodurch auch eine detaillierte Zugriffshistorie und sogar alte Versionen aus freien Speicherbereichen rekonstruiert werden könnten. Zudem könnten auch schon gelöschte Tagebücher wiederhergestellt werden, wobei die Daten insgesamt ohne Aufwand kopierbar sind. Doch es geht noch weiter, denn mit der Online-Durchsuchung sollen auch „die Aktivitäten des Nutzers protokolliert werden“,[265] also könnte dem Betroffenen direkt beim Schreiben des Tagebuchs über die Schulter gesehen werden. Der Denkprozess wäre fast direkt beobachtbar. Diese Möglichkeiten zeigen, dass das Verständnis von „Funden“ für die Analyse der Grundrechtsposition nicht einfach von der materiellen Welt übertragen werden kann.

Das Bedenkenswerte dieser Möglichkeiten ist nicht nur, dass all dies einfach machbar ist, sondern auch, dass der Betroffene von der Fülle der vorhandenen Informationen in der Regel nichts ahnt.[266]

Dieses Nichtwissen des Betroffenen umfasst auch die vielfältigen Metadaten und Logs eines informationstechnischen Systems. Sie reichen von Informationen, welche Kamera der Betroffene verwendet und wo er im Urlaub war, über detaillierte, langfristig gespeicherte Positions- und Bewegungsdaten,[267] sogenannte Caches (besondere Speicher zum temporären Vorhalten von vielgenutzten Daten) diverser Programme, Konversationsprotokolle, Suchworte in Suchmaschinen bis hin zu den gespeicherten Betriebszeiten des Systems; alles mit ausgedehnter zeitlicher Dimension. Dazu existieren vielerlei informationstechnische Werkzeuge, um diese komplex-heterogenen Daten zu analysieren, zu gruppieren, statistisch auszuwerten und Zusammenhänge zu finden; auch große Datenmengen sind mit diesen Instrumenten zu bewältigen.

[264] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort zu Frage 2.

[265] Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seite 6.

[266] Vergleiche Pfitzmann, *Rede vor dem Bundesverfassungsgericht als Sachverständiger zur Online-Durchsuchung*, 10.10.2007, Seite 4.

[267] Besonders bei mobilen Geräten, siehe Apple-Vorfall: Stegers, *Das iPhone als Spitzel*, 21.4.2011, aber durch WLAN-Ortung auch bei Desktopcomputern.

Durch die beiden Aspekte der dem Nutzer unbekannten Daten und der zeitlichen Ausdehnung geht eine Online-Durchsuchung — gerade auch im Hinblick auf zukünftige Entwicklungen der Informationstechnik — weit über das Durchsuchen im Schrank vergessener Briefpost hinaus, was den obigen Vergleich „Reise ins Unterbewusstsein des Betroffenen“ zusätzlich verdeutlicht.

Nutzungsverhalten

Zudem kann eine aktive Online-Durchsuchung gelesene Webseiten, geöffnete Dokumente, geschriebene (und wieder gelöschte) Texte, aufgenommene Videos, Film- oder Musikvorlieben und überhaupt alle Interaktionen mit dem informationstechnischen System überwachen[268] und auswerten. Es kann daher auch ermittelt werden, ob langsam gelesen oder schnell, ob Notizen gemacht oder gleich danach kommuniziert wurde. An dieser Stelle sei auf zahlreiche Literatur zum Thema Nutzungsverhalten und Nutzerdaten in informationstechnischen Systemen (auch bezogen auf das Internet) verwiesen.[269]

So bekommt die Frage, „was [...] die Zielperson bezogen auf ihr Informationssystem/ihren Rechner in der Vergangenheit gemacht“[270] hat und momentan tut, eine zukünftig unabsehbar vollständige Antwort.[271]

Der digitale Kernbereich

Dass die auf dem System vorhandenen Daten (im Sinne von Dateien) der Online-Durchsuchung zur Verfügung stehen, ist klar ersichtlich. Erwähnenswert ist hier noch einmal, dass aufgrund der heutzutage schon verfügbaren Datenträgergrößen viele Dokumente (z. B. Notizen, Bilder, E-Mails, etc.), die in der materiellen Welt aufgrund von Platzmangel oder Ordnungsliebe längst weggeworfen worden wären, nicht gelöscht werden und somit durch die ODS auch Jahre später noch auffindbar sind. Weiter finden sich unter den Daten informationstechnischer Systeme die Zugangsdaten zu Online-Diensten wie E-Mail-, Kalender- oder Kontaktdiensten, Online-Shopping-Plattformen, Online-Banking, eGovernment-Plattformen, Online-Festplatten und sozialen Netzwerken.[272] Zentral auffindbar durch die ODS in der komfortablen Passwortmerkfunktion des Browsers oder bei Eingabe direkt abgreifbar können diese Information nach § 110 Abs. 3 StPO zur weiteren Informationsbeschaffung verwendet werden.

Aus der Gesamtheit dieser Informationen kann regelmäßig ein fast vollständiges Bild der Persönlichkeit des Betroffenen abgeleitet werden; vom Arbeitsleben, Ortsbewegungen, familiären Verhältnissen, freundschaftlichen Beziehungen, persönlichen Notizen, politischen Einstellun-

[268] Vergleiche Unterabschnitt 3.1.6 (Datensuche).
[269] Siehe z. B. Kurz, „Die Geister die ich rief... Deine Spuren im Netz, Symposium 2007“, 2008 oder Schneier, *Secrets and Lies*, 2004, Seite 30 ff.
[270] Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seite 6.
[271] Vergleiche Bogk (Chaos Computer Club), *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007, Seite 13.
[272] Weiterführend Kurz, „Die Geister die ich rief... Deine Spuren im Netz, Symposium 2007“, 2008, Seiten 4 und 5.

gen bis hin zu intimsten Details von Lebensführung und höchstpersönlicher Gedankenwelt.[273] Eine Zusammenführung dieser Daten mit anderweitig beschafften Informationen ist durch ihre additiven Effekte — auch in zukünftiger Sicht — kaum abschätzbar. Oft sind auch private Daten anderer Personen betroffen, besonders bei Kommunikationsdaten; dort gibt es immer auch einen Kommunikationspartner, dessen Daten ebenso vorliegen.[274] Bei einer solch immensen Eingriffstiefe einer Maßnahme müssen für den Einsatz Vorkehrungen getroffen werden, damit der Kernbereich privater Lebensgestaltung auch im digitalen Zeitalter[275] geschützt bleibt.[276]
Das Gericht konkretisierte: „Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen".[277] Weiter hieß es: „In vielen Fällen wird sich die Kernbereichsrelevanz der erhobenen Daten vor oder bei der Datenerhebung nicht klären lassen".[278] Und zuletzt: „Entscheidende Bedeutung für den Schutz hat insoweit die Durchsicht der erhobenen Daten auf kernbereichsrelevante Inhalte, für die ein geeignetes Verfahren vorzusehen ist, das den Belangen des Betroffenen hinreichend Rechnung trägt."[279]
Im beschriebenen zweistufigen Prozess soll also ein „hinreichender" Schutz kernbereichsrelevanter Inhalte gewährleistet werden. Dies bedeutet in der Folge, dass, wenn eine Stufe (möglichst die erste, technische) dem Schutz stärker Rechnung trägt, die andere Stufe eventuell nur verhältnismäßig schwächer zu schützen braucht. Daher soll im Folgenden analysiert werden, wie ein technischer Kernbereichsschutz prinzipiell aussehen kann und wie viel er zum Ziel „Kernbereichsschutz" beitragen kann.

4.1.4 Technischer Kernbereichsschutz

Der Präsident des Bundeskriminalamtes Jörg Ziercke sagte am 19.10.2011 in Bezug auf die Quellen-TKÜ vor dem Innenausschuss, der „Kernbereichsschutz wird im Rahmen der inhaltlichen Auswertung mit Hilfe der Auswertesoftware gewährleistet"[280] und auch 2007 beantwortete das Bundeskriminalamt eine Frage nach der Suchstrategie schon ähnlich: „Das Verbot der Verwendung bestimmter Suchkriterien dient der Gewährleistung des grundrechtlich gebotenen Kernbereichsschutzes, indem nach derartigen Inhalten nicht gezielt gesucht werden darf".[281]

Wie könnten solche „Suchkriterien" aussehen, nach denen „Auswertesoftware" kernbereichsrelevante Informationen aussortieren würde?

[273] Vergleiche rechtliche Bewertung in Buermeyer, „Die Online-Durchsuchung. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme.", 2007, Seite 19 oder Strafrechtsausschuss der Bundesrechtsanwaltskammer, *Stellungnahme der Bundesrechtsanwaltskammer zur sogenannten Online-Durchsuchung*, März 2007, Seite 4.

[274] Siehe auch Bogk (Chaos Computer Club), *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007, Seite 13.

[275] Kurz, *Kernbereichsschutz*, März 2009.

[276] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 122.

[277] A.a.O. Absatz 281.

[278] A.a.O. Absatz 282.

[279] A.a.O. Absatz 283.

[280] Ziercke, *Sprechzettel für die Teilnahme des Präsidenten des Bundeskriminalamtes Jörg Ziercke an der 53. Sitzung des Innenausschusses zu TOP 24a (24b, 24c)*, 19.10.2011, Seite 7.

[281] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort auf Frage 7.

Moderne digitale informationstechnische Systeme sind im Grundprinzip Symbolmanipulatoren, sie können — einfach ausgedrückt — nach formalen Regeln Operationen auf Symbolen ausführen, z. B. Symbole vergleichen und abhängig vom Ergebnis andere Symbole nach formalen Regeln verändern.[282] Jede Information und auch die Regeln selbst müssen in der Symbolsprache des informationstechnischen Systems kodiert sein, damit die Symbolregeln korrekt auf die Symbole angewendet werden können. Welche Informationen die Symbole kodieren und welche Überlegungen den Regeln zugrunde liegen, ist für die Operation des informationstechnischen Systems irrelevant, es arbeitet die Regeln einfach formal korrekt ab. Texte lassen sich durch den digitalen Charakter von Buchstaben[283] sehr einfach kodieren (bei analogen, also kontinuierlichen Inhalten wie Bild- oder Tondaten muss erst noch Quantisierungsarbeit betrieben werden, damit sie in ein Kodierungsschema passen[284]). Wichtig ist hier, dass auch die Regeln formal kodiert werden müssen, sei es ein Computerprogramm oder die Suchkriterien für Inhaltsfilter. Darin ist begründet, dass digitale informationstechnische Systeme nur syntaktisch (bei Texten z. B. auf Zeichenbasis, bei Bild- und Tondaten auf Musterbasis) suchen können. Um also kernbereichsrelevante Inhalte filtern zu können, müsste „Kernbereichsrelevanz“ abschließend definiert und formalisiert werden. Gerade das kann als unlösbar bezeichnet werden, zumal es kein primär technisches Problem ist.[285] Die Filterung nach kernbereichsrelevanten Inhalten wird also viel zu viele, viel zu wenige oder einfach die falschen Daten als kernbereichsrelevant ausblenden. Gleiches gilt für andere Suchkriterien wie Speicherort, Dateiformat, Datum oder Datenquelle (Audio, Video, Scanner etc.). Klarer wird das Problem auf ganz praktische Weise, indem man selbst versucht, Schlüsselbegriffe zur Erkennung von Kernbereichsrelevanz zu erdenken, wenn — so der ehemalige Bundesinnenminister Schäuble — auch Tagebücher Terroristeninformationen enthalten können.[286]

Sieht man diese Ereignisse im Lichte nachrichtendienstlicher oder ermittlungsbezogener Informationsbeschaffung, bei der keine Hinweise übersehen werden sollen, wird auch die rechtliche Ausgestaltung eines Kernbereichsschutzes klar. Im Urteil zum großen Lauschangriff hieß es: „Sollte im Rahmen einer Wohnraumüberwachung eine Situation eintreten, die dem unantastbaren Kernbereich privater Lebensgestaltung zuzurechnen ist, muss die Überwachung abgebrochen werden“.[287] Bei kernbereichsschützenden Passagen wie §20k Absatz 7 (Online-Durchsuchung) und BKAG §20l Absatz 6 (Quellen-TKÜ), die die Maßnahme nur dann als unzulässig verbieten, wenn angenommenermaßen ausschließlich Inhalte aus dem Kernbereich privater Lebensgestaltung erhoben würden, ist die Motivation zwar erkennbar, für eine tatsächlichen Schutzwirkung sind sie jedoch gänzlich ungeeignet;[288] bei einer automatisierten

[282] Hedtstück, *Einführung in die theoretische Informatik*, 2007, Seite 5 ff.
[283] Vergleiche Goodman, *Languages of Art*, 1976, Ende Kapitel IV.
[284] Klimant, Piotraschke und Schönfeld, *Informations- und Kodierungstheorie*, 2006, Seite 33 ff.
[285] Siehe auch Hansen und Krause, *Heimliche Online-Durchsuchung – Wie geht's, wie schütze ich mich?*, 2007, Seite 35 oder Köhntopp und Köhntopp, *Why Internet Content Rating and Selection does not work*, 1999.
[286] Rath, *"Terroristen sind auch klug"*, 8.2.2007.
[287] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum großen Lauschangriff*, 3.3.2004, Absatz 152.
[288] Siehe dazu Geiger, *Stellungnahme zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt BT-Drucksache 16/9588*, August 2008, Seite 3 und Schaar, *Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Gesetzentwurf der Fraktionen der*

Erhebung durch eine Online-Durchsuchung/Quellen-TKÜ mit der weiter oben beschriebenen technischen Unmöglichkeit einer brauchbaren Vorfilterung sollen so viele Daten wie möglich erhoben werden.

Diese Verschiebung des Kernbereichsschutzes von einem Verbot der Datenerhebung zu einem Verbot der Datenverwertung nach Durchsicht[289] ist technisch bedingt und hebt genau dadurch den absoluten Charakter des Kernbereichsschutzes auf. Anders ausgedrückt ist die neue Kernbereichsbestimmung das fragwürdige Ergebnis einer technikabhängigen Abwägung.[290]

Letztendlich muss die Aussage „Der Schutz des Kernbereichs anderer Benutzer wie auch des Beschuldigten kann allein mit technischen Mitteln nicht abschließend garantiert werden“[291] umformuliert werden in: Der Schutz des Kernbereichs anderer Benutzer wie auch des Beschuldigten kann allein mit technischen Mitteln nicht einmal ansatzweise sichergestellt werden.[292]

Zur Ausgangsfrage dieses Abschnitts zurückkommend muss also festgehalten werden, dass technisch nicht nach Kernbereichsrelevanz vorgefiltert werden kann. Die zweite Stufe der Gewährleistung des Kernbereichsschutzes — die Durchsicht — muss die Gewährleistung daher sehr, sehr ernst nehmen. Zu diskutieren ist daher, ob es den Belangen des Betroffenen hinreichend Rechnung trägt, wenn die Gewährleistungsverantwortung allein und gänzlich der ausforschenden Stelle obläge.

4.1.5 Missbrauchspotenzial

Das Missbrauchspotenzial dieser Maßnahme ist sehr groß, sowohl durch den Vollzugriff auf das System des Betroffenen als auch durch die zu sammelnden und auszuleitenden Daten, die ohne Aufwand kopierbar in den ausforschenden Stellen sowie bei externen Datenauswertungsdienstleistern — und somit Dritten — vorliegen. Umstritten ist, ob die Dokumentationspflichten für die Datenweitergabe in Deutschland überhaupt ausreichend geregelt sind.[293] In einigen Fällen sind die zur Auswertung vorgesehenen Datenträger einfach verlorengegangen und später Sicherungskopien davon an anderer Stelle wieder aufgetaucht,[294] oder es wurden erlangte Daten für private Zwecke missbraucht.[295]

Die gänzliche Verfügbarkeit aller Daten und Zugangsdaten, die Möglichkeit der „Online-Kontrolle“ des infiltrierten Systems und die prinzipielle Unmöglichkeit der Nachvollziehbarkeit der

CDU/CSU und der SPD: Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, BT-Drs. 16/9588, 15.9.2008, Seiten 4 und 5.

[289] Vergleiche Krempl und Ziegler, *Noch viele Fragen offen bei heimlichen Online-Durchsuchungen*, 15.9.2008.

[290] Vergleiche den ursprünglichen Ansatz der Bestimmung des Kernbereichs Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum Tagebuchinhalt I*, 14.9.1989, Absatz 48.

[291] Bundesministerium des Innern, *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, 22.8.2007, Antwort zu Frage 5.

[292] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 278.

[293] Kurz, *Kernbereichsschutz*, März 2009, Seite 9.

[294] O. V. *Verschwundene Festplatte offenbar noch in Kopie vorhanden*, 26.4.2000.

[295] Stark, „Digitale Spionage“, 2009.

ODS-Aktivitäten[296] öffnet dem Missbrauch Tür und Tor. Unter Missbrauch fällt hier auch die zweckfremde Nutzung der Daten[297] oder eine Schädigung des Betroffenen durch Bekanntwerden von Informationen über ihn.[298] Bislang besteht der „Schutz“ der Betroffenen während der Maßnahme darin, dass „das systemtechnische Protokoll [...] aus der Bedienoberfläche heraus nicht (von den Beamten, Anm. d. Verfassers) manipulierbar“[299] ist. Die Bedienoberfläche ist jedoch nur die „Vordertür“ und eine Sicherung dieser bedeutet keinesfalls die Sicherheit des restlichen Systems.
Vermutlich wird diese Schutzvorkehrung oder die gesamte Maßnahme mit der nächsten Generation Kriminalbeamter überarbeitet werden müssen.[300] Danach liegen die Daten, wie oben beschrieben, bei der auswertenden Stelle. Das Missbrauchspotenzial ist nicht deshalb so einzigartig hoch, weil sich mehr schwarze Schafe in diesem Bereich der Exekutive tummeln als woanders oder weil die Menschen dort mehr Fehler machen[301] — darüber kann der Autor keine Aussage treffen, sondern weil regelmäßig die gesamte digitale Persönlichkeit eines oder mehrerer Betroffener in einem kleinen Datenträger oder Gerät konzentriert vorliegt und zur Gänze verfügbar ist.

4.1.6 Gefährdung für Dritte

Von einer derartig eingriffsintensiven Maßnahme gehen auch Risiken aus, die nicht nur die Zielperson selbst betreffen. Damit sind nicht nur die Daten Dritter gemeint, die auch auf dem informationstechnischen System der Zielperson in Form von E-Mails oder Fotos zu finden sind, sondern auch informationstechnische Systeme unbeteiligter Dritter. Dabei ist zu bedenken, dass ein informationstechnisches System sich über mehrere physische Geräte erstrecken kann (z. B. die Daten einer Person auf seinem lokalen System und einem gemieteten Internetserver) und dass ein physikalisches Gerät eine Vielzahl informationstechnischer Systeme beinhalten kann (z. B. ein Mailserver, der von vielen Benutzern genutzt wird). Informationstechnische Systeme unbeteiligter Dritter können in Mitleidenschaft gezogen werden, wenn andere Systeme als das Zielsystem infiltriert werden oder wenn das infiltrierte System Teile der informationstechnischen Systeme Dritter umfasst; eine Kombination der beiden ist denkbar.
Die Gefahr der Infiltration anderer Systeme als des Zielsystems hängt sehr stark von der Einbringungsmethode ab. Das Auslegen von CDs oder USB-Sticks, das Versenden präparierter E-Mailanhänge oder Links zu präparierten Webseiten bergen ein hohes Risiko einer Infiltration vieler fremder Systeme.

[296] Siehe Abschnitt 3.3 (Fehlende Protokollierbarkeit) und Unterabschnitt 4.2.4 (Aussagekraft von Daten mit extrinsischer Personenbeziehbarkeit).

[297] Vergleiche Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Seite 122.

[298] Sieber, *Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen*, 9.10.2007, Seite 18.

[299] Ziercke, *Sprechzettel für die Teilnahme des Präsidenten des Bundeskriminalamtes Jörg Ziercke an der 53. Sitzung des Innenausschusses zu TOP 24a (24b, 24c)*, 19.10.2011, Seite 8.

[300] „Die allermeisten unserer Kolleginnen und Kollegen wurden zu einer Zeit ausgebildet, als es weder Computer noch ein Internet gab.“ aus Borchers und Kuri, *Kriminalbeamte fordern Verstärkung am digitalen Tatort*, 27.10.2011.

[301] Dazu auch Pfitzmann, *Rede vor dem Bundesverfassungsgericht als Sachverständiger zur Online-Durchsuchung*, 10.10.2007, Seite 1.

Wie sehr es vermieden werden sollte, andere Systeme zu infiltrieren, zeigt folgende Aussage: „Insbesondere verdeckt agierende Programme (z. B. Rootkits) sind schwer wieder vollständig zu entfernen, da sie notwendigerweise tief in die Abläufe des Betriebssystems eingreifen. Üblicherweise muss nach der Infektion durch eine Spionagesoftware das gesamte Betriebssystem mitsamt der Anwendungssoftware von Grund auf neu installiert werden“.[302] Durch die tiefe Verwurzelung in und die notwendige Interaktion mit dem fremden System sowie die Komplexität der zu erfüllenden Funktionen ist das Verhalten der ODS auf dem System generell sehr schwer vorhersagbar; zusammen mit der fehlenden Testphase sind regelmäßig Fehler in der Software zu erwarten. Bestenfalls äußern sich die Fehler in marginaler Funktionsstörung der ODS, im schlimmsten Fall verändert die ODS das System so, dass nicht sofort Abstürze oder Fehler offensichtlich werden, aber im Hintergrund Daten auf lange Sicht korrumpiert werden. Diese Art und Intensität technischer Eingriffe wird beim System der Zielperson in Kauf genommen, weil es einer gesetzlich ermächtigten (den potenziellen Schaden miteinbeziehenden) Informationsgewinnung dient, bei unbeteiligten Dritten aber ist eine versehentliche Infiltration unverantwortlich. Hinzu kommt, dass bei Angriffen auf ein System erst nach einer ersten Auswertung erhobener Daten sicher festgestellt werden kann, ob das gewünschte System infiltriert wurde.[303] Der Grundrechtseingriff findet also in diesem Fall vor der korrekten Identifikation des Zielsystems statt.
Hier muss das Augenmerk auch auf großflächige Effekte gelegt werden. Wird die Software für den Einzelfall speziell konfiguriert, so dass sie auf keiner anderen Konfiguration laufen kann, ist eine unabsichtliche Verbreitung sehr unwahrscheinlich,[304] ist sie aber z. B. auf allen Microsoft Windowsversionen lauffähig, müssen derartige Verbreitungsgefahren unbedingt verhindert werden. Einzig durch die direkte Aufbringung der ODS auf das System kann die Zielproblematik sicher gelöst werden.

Auswirkungen auf das Internet

Für den Fall, dass das infiltrierte System Dienste für Dritte bereitstellt, kann es auch zur Infiltration weiterer informationstechnischer Systeme kommen.[305] Im Falle von Peer-to-peer-Netzwerken können die Nutzer wahrscheinlich nicht „den Umständen nach davon ausgehen (dass sie darüber) selbstbestimmt verfüg(en)“,[306] aber „je nach Fallkonstellation können auch Server von der Online-Durchsuchung umfasst werden.“[307] Dies würde eine ganze Menge Probleme mit sich überschneidenden informationstechnischen Systemen verschiedener Nutzer mit sich bringen:
Der Zielrechner könnte File-/Web-/Mail-/Cloudserver oder Hypervisor für virtuelle Maschinen sein, jeder mit den Daten vieler Nutzer und somit vieler Betroffener. Die Eintrittswahrschein-

[302] Freiling, *Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, 27.9.2007, Seite 7.
[303] Chaos Computer Club, *QUELLEN-TKÜ-Stellungnahme des Chaos Computer Clubs*, 2009, Seite 17.
[304] Weiterführend Fox, *Stellungnahme zur „Online-Durchsuchung“, Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, 29.9.2007, Seite 15.
[305] Bogk (Chaos Computer Club), *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007, Seite 17.
[306] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 206.
[307] Bundesministerium des Innern, *Fragenkatalog des Bundesministeriums der Justiz*, 22.8.2007, Seite 3.

lichkeit dieser Art von Fehlinfiltration ist jedoch als gering einzuschätzen, weil solcherart Server eher gut gesichert[308] und anders aufgebaut sind (oder sein sollten), doch im Lichte des potenziellen Eingriffs muss auch hier auf die direkte Aufbringung als sichere Vermeidungsstrategie gegen Kollateralschäden verwiesen werden.

Weite Kreise

Da, wie bereits oft geschehen, Bundesbehörden (in diesem Falle der Bundesnachrichtendienst als Amtshilfe)[309] auf dem „Schwarzmarkt" Sicherheitslücken bzw. deren Exploits erstehen, muss auf dessen besondere Folgen hingewiesen werden:

Erstens rücken Bundesbehörden mit derartigen Machenschaften näher zu kriminellen Kreisen und organisierter Kriminalität, unterstützen diese durch den Kauf von Software und sorgen letztlich für eine Ausweitung und in gewissem Sinn auch für die Legitimation jener Märkte. Dieser Umstand ist für Geheimdienste schon besorgniserregend genug, aber wenn Amtshilfe für andere gefahrenabwehrende Bundesbehörden dazukommt, muss die Frage rechtsstaatlicher Handlungsprinzipien gestellt werden, zumal die Einsatzhäufigkeit der Online-Durchsuchung zunehmen wird. Strittig ist auch, ob in solchen Fällen auch der sogenannte Hackertoolparagraph (§ 202c StGB bzw. 303 a, b StGB) zum Tragen kommen kann.[310]

Die Vergrößerung des Exploitmarktes unterstützt aber nicht nur kriminelle Organisationen in zunehmenden Maße, sondern schadet auch indirekt der Allgemeinheit, denn so werden Sicherheitsprobleme in Zukunft wohl eher den Geheimdiensten oder Exploithändlern angeboten, als sie den Herstellern mitzuteilen oder sie zu veröffentlichen. Dadurch entsteht ein Schaden durch Unterlassen, also die Nichtveröffentlichung von Sicherheitslücken,[311] an der informationstechnischen Welt, dem die Gründung des Bundesamtes für die Sicherheit in der Informationstechnik (BSI)[312] eigentlich entgegenwirken soll.

Wird dieser Weg weiter beschritten (insbesondere mit Amtshilfe durch Geheimdienste), werden ein Zielkonflikt der staatlichen Vorgehensweisen (informationstechnische Systeme sicherer zu machen einerseits und sie gut infiltrieren zu können andererseits) und vielleicht noch schlimmer, der Vertrauensverlust des Bürgers in rechtsstaatliches Handeln die Folge sein.[313] Eine Evaluation der Einhaltung des Trennungsgebotes von Polizei und Geheimdienst scheint in dieser Hinsicht ebenso nötig.[314]

---

[308] „Bei professioneller Beachtung aller Sicherheitsvorkehrungen ist also davon auszugehen, dass das Aufbringen eines Trojaners scheitern wird" in Bogk (Chaos Computer Club), *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007, Seite 12, siehe auch Fox, *Stellungnahme zur „Online-Durchsuchung", Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, 29.9.2007, Seite 11.

[309] Pohl, „Zur Technik der heimlichen Online-Durchsuchung", 2007, Seite 687.

[310] Vergleiche Wegener, *Vortrag: Hackerparagraph und Online-Durchsuchung*, 8.5.2008.

[311] Fox, *Stellungnahme zur „Online-Durchsuchung", Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, 29.9.2007, Seite 15.

[312] Das Bundesamt für Sicherheit in der Informationstechnik, *Aufgaben des BSI*, 2011.

[313] Pohl, „Zur Technik der heimlichen Online-Durchsuchung", 2007, Seite 687.

[314] Vergleiche Roggan, „Legalisierung im Polizei- und Geheimdienstrecht", 2008.

4.2 Erkenntnisgewinn der Funde

Bislang waren technische Gestaltung/Aufwand, Seiteneffekte, Grundrechtseingriff, gesellschaftliche Einordnung und die Risiken Gegenstand dieser Arbeit. Im Folgenden soll nun der Nutzen der Maßnahme und, weil es eine Informationsbeschaffungsmaßnahme ist, der Nutzen der gewonnenen Informationen und Erkenntnisse betrachtet werden.

4.2.1 Exkurs: Computerforensik

Da die Online-Durchsuchungs-Software forensikähnliche Aufgaben erledigen soll, werden „bei der Entwicklung [werden] besonders die Aspekte der Gerichtsverwertbarkeit der Ergebnisse [...] berücksichtigt".[315] Um den Charakter der Informationen und Erkenntnisse richtig einordnen zu können, ist es hilfreich, sich kurz mit den Grundlagen aktueller Methoden und Abläufe der Computerforensik zu beschäftigen. Die Computerforensik als Teil der Forensik beschäftigt sich mit dem „methodischen[s] Vorgehen zur Aufklärung von Straftaten unter Verwendung von IT-Systemen".[316]

Idealerweise läuft die computerforensische Analyse z. B. eines Datenträgers wie folgt ab:[317]

I. Sicherstellung Zunächst werden entweder nur Datenträger oder der gesamte Computer sichergestellt. Gegebenenfalls wird die Stromversorgung des Systems direkt gekappt, damit beim Herunterfahren keine Daten gelöscht oder verändert werden können. Die beschlagnahmte Hardware wird dann sachverständigen Kriminaltechnikern zur Analyse gegeben.

II. Schreibschutz Dann wird der Datenträger ggf. aus dem Computer entfernt und über einen Schreibblocker mit dem Analysesystem verbunden. Dadurch wird hardwarebasiert sichergestellt, dass nur lesend auf die Datenträger zugegriffen werden kann.

III. Imagekopie Vom Analysesystem aus wird der Datenträger nun zur Gänze ausgelesen und als Image (exakte Bitkopie) gespeichert. Dieses Image umfasst den gesamten Datenbereich des Datenträgers inklusive freiem Speicher, damit später z. B. auch versteckte Dateien und Partitionen gefunden werden können.

IV. Kryptographische Prüfsumme Über das Image wird sofort eine kryptographische Prüfsumme errechnet, damit das erzeugte digitale Image als „Original" identifiziert werden kann. Jegliche Untersuchung wird nur an diesem Image durchgeführt, nie am Original-Datenträger.

V. Eigentliche Untersuchung Jetzt kann die eigentliche Untersuchung der Daten stattfinden, wobei nach jedem eventuellen Änderungsschritt eine neue kryptographische Prüfsumme

[315] Bundesregierung der 16. Wahlperiode, *Drucksache 16/4997*, 10.4.2007, Antwort zu Frage 4.
[316] Bundesamt für Sicherheit in der Informationstechnik, *Leitfaden „IT-Forensik"*, 2011, Seite 9.
[317] Vergleiche Geschonneck, *Computer-Forensik*, 2011, Seite 91 ff. und Bundesamt für Sicherheit in der Informationstechnik, *Leitfaden „IT-Forensik"*, 2011, Seite 89 ff.

erzeugt wird, so dass er mit der erstellten Dokumentation transitiv ausgehend vom Originalimage nachvollzogen werden kann.

VI. Vorlage der Ergebnisse Durch die lückenlos nachvollziehbare Dokumentation halten die Funde Gutachterprüfungen stand und können bei Gericht verwendet werden.

Wird dieses „streng methodische, jederzeit nachweisbare und begründbare Vorgehen während einer forensischen Untersuchung“[318] nicht eingehalten, ist eine Zulassung der Funde vor Gericht unwahrscheinlich.[319] Werden in solchen Untersuchungen vermeintlich relevante Daten gefunden, besteht der nächste Schritt darin, die Zuordnung zu einer Person vorzunehmen.

4.2.2 Zuordnung zu Personen

Sichergestellte Daten haben — genauso wie sichergestellte physische Dinge — grundsätzlich erst einmal keinen Personenbezug. Einer Jacke z. B. ist nicht „anzusehen“, wem sie gehört. Wird sie jedoch bei einer Hausdurchsuchung im Zimmer einer Person gefunden, ist dies Grund für die Annahme, dass diese Jacke (zu) der Person gehört. Wurde diese Jacke nun irgendwo anders gesehen, kann wiederum eine Verbindung zur Person konstruiert werden.
Im Digitalen verhält es sich ähnlich, nur dass z. B. der räumliche Aspekt nicht exakt so vorhanden ist; dafür gibt es andere teilweise ähnliche Merkmale, wie z. B. den Auffinde„ort“ oder die oben beschriebenen Rechteidentitäten. Wenn Daten auf einem Datenträger gefunden werden, könnte der Personenbezug mit den Antworten auf folgende Fragen konstruiert werden: 1) Welcher Rechteidentität waren die Daten zugewiesen? 2) Welche Person hat das System unter dieser Rechteidentität verwendet? 3) Lassen Systemkonfiguration und Systemzustand den Schluss zu, dass wahrscheinlich auch keine systeminternen Vorgänge diese Daten erzeugt oder verändert haben können?
Der erste Schritt wird anhand des schreibgeschützten Datenträgerimages technisch gelöst, der zweite Schritt kann mit technischen Mitteln in diesem Fall nicht gelöst werden,[320] jedoch können andere nichttechnische Ermittlungsmethoden verwendet werden, was für normale Ermittlungen jedoch selten problematisch ist, wenn der Datenträger z. B. durch Hausdurchsuchung privater Räume erlangt wurde. Der dritte Schritt verlangt wieder IT-forensische Methoden. Dazu findet eine entsprechende Datenträger-/Systemanalyse statt. Kommt der Forensiker dabei zu der Auffassung und kann diese belegen, dass das System nicht in seiner Integrität beeinträchtigt war, also nicht befallen von Trojanischen Pferden, Rootkits, Viren oder Würmern, die die Möglichkeit gehabt hätten, entsprechende Daten zu produzieren, kann die Zuordnung zur Person angenommen werden.[321] Ergibt die Analyse aber, dass die Integrität des Systems verletzt war und „fremde“ Programme darauf aktiv gewesen sein könnten, um Daten unter dieser Rechteidentität zu produzieren, ist es nicht ohne weiteres „möglich [...], logisch nachvoll-

[318] A.a.O. Seite 9.

[319] Hansen und Krause, *Heimliche Online-Durchsuchung – Wie geht's, wie schütze ich mich?*, 2007, Minute 6:40, siehe auch das „Faxurteil“ Amtsgericht Lübeck Az: 63 Ds 706 Js 101113/03 (579/03), wo den Funden deswegen kein Beweiswert zugesprochen wurde.

[320] Fox, *Stellungnahme zur „Online-Durchsuchung“, Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, 29.9.2007, Seite 13.

[321] Für den interessierten Leser empfiehlt der Verfasser z. B. Blenkers, *Tatort Internet*, 22.8.2011.

ziehbare Verbindungen zwischen Ereignissen und Beweisspuren und evtl. auch an Personen herzustellen".[322]

4.2.3 Extrinsische Personenbeziehbarkeit und intrinsischer Personenbezug

Die Personenzuordnung bei der Online-Durchsuchung ist ungleich schwieriger. Hier muss durch den entfernten Charakter der Online-Durchsuchung eine Verbindung von aus dem Internet im ODS-Kontrollzentrum empfangenen Daten zu einer Person konstruiert werden. Es muss also belegt werden, dass die ODS vom richtigen System aus Daten versendet hat, die sie auch dort so gefunden hat.

An dieser Stelle kann man zwei Aspekte des Personenbezugs von Daten unterscheiden. Einerseits die extrinsische Personenbeziehbarkeit, die bei digitalen schriftbasierten Daten (E-Mails, Texte, Dokumente), Binärdateien oder GPS-Logfiles den Hauptaspekt darstellt, und andererseits der intrinsische Personenbezug, der bei „analogen" Fotos, Videos bzw. Tonaufnahmen (wenn sie Personen zeigen bzw. deren Stimmen wiedergeben, so dass diese identifiziert werden können) hervortritt.[323]
Wird z. B. ein beliebiges Textdokument auf dem informationstechnischen System von Person A entdeckt, wäre die erste Personenzuordnungsvermutung des Inhalts „Person A", würde das gleiche Textdokument jedoch auf dem informationstechnischen System von Person B entdeckt, wäre die erste Personenzuordnungsvermutung des Inhalts dagegen „Person B". Die Personenzuordnung basiert folglich auf Informationen, die *nicht* in den Daten selbst kodiert sind; die Daten sind nur extrinsisch personenbeziehbar.
Wird andererseits z. B. ein Video, das Person A zeigt auf dem informationstechnischen System von Person A entdeckt, wäre die erste Personenzuordnungsvermutung des Inhalts „Person A", würde das gleiche Video jedoch auf dem informationstechnischen System von Person B entdeckt, wäre die erste Personenzuordnungsvermutung des Inhalts trotzdem „Person A". Die Personenzuordnung basiert im Videofall auf Informationen, die tatsächlich in den Daten selbst kodiert sind; sie sind also intrinsisch personenbezogen.

Der Grund für das Hervorheben dieser Unterscheidung ist, dass die Änderung von Personenbeziehbarkeitsinformationen extrinsisch personenbeziehbarer Daten gänzlich und einfach mit ODS-Mitteln möglich ist. Es ist ersichtlich, dass für derartige erhobene Daten die vollständige Kette (System -> ODS -> Internet -> Kontrollzentrum) mit technisch realisierten Echtheitsbelegen abgesichert werden muss, damit sie einen Personenbezug und somit erst Beweiswert erhalten können.
Bei Daten mit intrinsischem Personenbezug kann man den Personenbezugsprozess möglicherweise etwas abkürzen. Nur möglicherweise und nicht komplett, da die Personenbezugsaspekte nicht unabhängig voneinander auftreten. Dass bestimmte Daten mit intrinsischem Personenbezug überhaupt auf einem System vorhanden sind, ist an sich schon ein extrinsisches Merkmal der Daten, dessen Beeinflussung im Aktionsbereich einer ODS liegt.

[322] Bundesamt für Sicherheit in der Informationstechnik, *Leitfaden „IT-Forensik"*, 2011, Seite 24.
[323] Anschaulich hierzu Schneier, *Secrets and Lies*, 2004, S. 74-75.

Darüber hinaus bedeutet intrinsischer Personenbezug nicht, dass die Personenbezugsinformationen nicht verändert worden sind,[324] doch die Fälschungsumstände und der Informationswert dieses Aspektes der Daten liegen anders begründet und haben eine eigene, der ODS nicht zugängliche Qualität.[325] Die Ausführung des Unterschieds würde den Rahmen dieser Arbeit sprengen, daher wird an dieser Stelle einfach mit der Unterscheidung der beiden Aspekte und deren Konsequenzen für den Personenbezug weitergearbeitet. Zunächst wird die Belegkette von Daten mit vornehmlich extrinsischer Personenbeziehbarkeit betrachtet.

Alle Aktivitäten der ODS finden auf einem fremden System statt. Das bedeutet, dass die ODS weder exklusiven Zugriff darauf hat — siehe Abschnitt 3.3 (Fehlende Protokollierbarkeit), noch dass sie dem System Daten vorenthalten kann, auf die sie selbst zugreifen kann oder muss. Der Programmcode und eventuelle Konfigurationsdateien müssen für das Betriebssystem lesbar vorliegen, nur so kann die ODS überhaupt ausgeführt werden. Sollte eines von beiden verschlüsselt gewesen sein, befinden sich notwendigerweise auch die Entschlüsselungsroutine und der Schlüssel im Speicher.
Sollte in der ODS ein hohes Maß an kryptographischen Mitteln verwendet worden sein, um Abläufe oder Daten zu sichern, müssen der ODS die entsprechenden Schlüssel mitgegeben worden sein. Die der ODS bekannten Geheimnisse (z. B. Schlüssel) werden also mit ausgeliefert. Damit wurden sie automatisch auch mindestens dem Betriebssystem des infiltrierten Systems und anderen Programmen auf dieser Ebene zugängig gemacht. Doch diese Schlüssel können nicht nur ausgelesen (und verwendet), sondern auch verändert werden, denn auch Selbsttests und dazugehörige Referenzwerte der ODS sind vor dem Betriebssystem nicht zu verbergen.

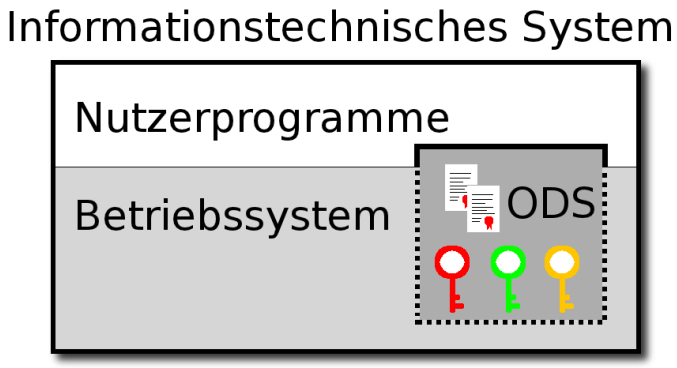


Abbildung 5: Position der ODS im System: Das Betriebssystem hat Zugriff auf alle Schlüssel, auch schreibend

Die Möglichkeiten der Software sind detailliert in Unterabschnitt 3.1.4 (Verankerung im System) und Unterabschnitt 4.1 (Einordnung und Auswirkungen der technischen Möglichkeiten der Software) behandelt worden, und auch auf die Suchmethoden und -möglichkeiten wurde weiter oben eingegangen, doch für die Analyse der Gerichtsfestigkeit der Daten muss auch

[324] Siehe dazu cristop5, *IPCC's Ben Santer admits GW hoax*, 17.8.2011.
[325] Weiterführend siehe Goodman, *Languages of Art*, 1976, Kapitel V.

auf eine eventuelle Datenmanipulation eingegangen werden. Bei allen Daten muss abgesichert werden, dass sie nicht von Viren, Trojanern, Würmern und anderer Malware dort platziert worden sind.[326] Durch Überlagerungen der Polizeiarbeit mit den Tätigkeiten der Nachrichtendienste[327] ist sogar ein „Doppelbefall" denkbar, falls zwei staatliche Stellen unabhängig voneinander das gleiche Zielsystem infiltrieren. Um diese Art Außenbeeinflussung des Systems auszuschließen, müssten kontinuierlich mannigfaltige Systemdaten überwacht und mit den Funden gespeichert werden. Die Erfolgsaussichten einer Aufdeckung solcher Umstände, auch noch im Nachhinein, sind allerdings sehr schlecht. An den Funden könnten somit in besonderen Situationen deswegen Zweifel angemeldet werden, das sollte jedoch nicht regelmäßig der Fall sein.

4.2.4 Aussagekraft von Daten mit extrinsischer Personenbeziehbarkeit

Um die Aussagekraft der von der ODS gewonnenen Daten zu analysieren, müssen zwei zeitlich versetzte Situationen untersucht werden. Erstens werden die Daten betrachtet, die als Funde der ODS auf dem infiltrierten System liegen, und zweitens die Daten, die als Funde beim ODS-Kontrollzentrum eintreffen.

Funde der ODS, die sich noch auf dem System befinden

Wie in Unterabschnitt 3.1.7 (Speicherung und Übermittlung der Funde) beschrieben, durchsucht die ODS das Zielsystem und speichert die Funde verschlüsselt in einem freien Bereich des Systems, bis eine Übermittlung möglich ist. Funde werden mit Schlüsseln verschlüsselt, die die ODS „bei sich" haben muss und zu denen, wie bereits beschrieben, auch das zu durchsuchende und zu überwachende System Zugriff hat. Jegliche Daten, die sich als „Funde" auf dem System befinden, können dort direkt als „Funde" platziert worden sein. Dies ist deswegen möglich, weil die Schlüssel auch dem System bekannt sind, nicht nur der ODS.

Wenn vermeintliche von einer ODS gefundene Daten nicht mehr auf einem System gefunden werden können, wird man annehmen, dass der Betroffene die Originaldaten in weiser Voraussicht absichtlich gelöscht hat, um Beweise zu vernichten. So würde den künstlich platzierten Funden sogar noch höherer Belastungswert zugeschrieben werden, als wenn die Daten ohne Wissen des Betroffenen einfach so auf dem System platziert worden wären.[328]

Unter diesen Umständen könnte nur ein Protokoll der ODS-Aktivitäten Klarheit darüber schaffen, ob diese Daten wirklich von der ODS gefunden oder extern „als Funde" platziert worden sind. Weil eine glaubhafte Protokollierung nicht möglich ist, kann jedoch nicht einmal ausgeschlossen werden, dass die ODS die Daten erst (versehentlich) selbst platziert und dann ganz offiziell gefunden hat.

---

[326] ap (The Associated Press), *Viruses Frame PC Owners for Child Porn*, 9.11.2009.

[327] Geiger, *Stellungnahme zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt BT-Drucksache 16/9588*, August 2008, Seite 1.

[328] Fox, *Stellungnahme zur „Online-Durchsuchung", Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, 29.9.2007, Seite 15.

Vom ODS-Kontrollzentrum empfangene Funde

Wenn im ODS-Kontrollzentrum der ausforschenden Behörde Funde von Online-Durchsuchungen eintreffen, muss davon ausgegangen werden können, dass diese Funde durch korrekt verwendete Verschlüsselungs- und Signierungsmethoden vom infiltrierten System kommen.[329] Dass die vom Zielsystem kommenden Daten nicht glaubwürdig sind, wurde soeben ausgeführt, doch im Kontrollzentrum ankommende Daten müssen nicht einmal vom Zielsystem versendet worden sein.
Alle Identifikationsdaten der ODS sind auf dem Zielsystem vorhanden und kopierbar, somit können Daten auch von anderen Systemen aus als „Funde vom Zielsystem" zum ODS-Kontrollzentrum geschickt werden. Es verursacht schon einen gewissen Aufwand, das Kommunikationsprotokoll der ODS zu dekonstruieren, aber durch die Möglichkeit der Beobachtung der ODS in operandi ist es trotzdem verhältnismäßig einfach möglich. Zwar zeigen die aktuellen Geschehnisse um den Staatstrojaner,[330] dass die momentan verwendeten Versionen minderwertige Produkte sind, aber auch bei korrekter Verwendung und Implementation starker kryptographischer Methoden ist der Sachverhalt des Fremdsendens nicht zu verhindern. Das grundlegend-prinzipielle Problem bleibt die Auslieferung aller nötigen Schlüssel in der ODS an das fremde System. Dies ist für den Einsatz von Kryptographie notwendig, das Problem ist daher nicht lösbar.

Weder die Daten, die bei der ausforschenden Stelle ankommen, weil sie von der ODS übermittelt worden sind, noch die von der ODS „archivierten" Funde, die bei einer etwaigen Konfiszierung des Systems der Zielperson gefunden werden könnten, würden einer genauen gerichtlichen Prüfung standhalten.[331] Dieses Problem ist informationstechnischen Ursprungs und prinzipiell nicht mit kryptographischen Mitteln lösbar. Mehr noch, die Infiltration des Systems durch eine Online-Durchsuchung zerstört gerade durch die Infiltration zusätzlich den forensischen Wert der restlichen Daten des Systems.[332]

4.2.5 Aussagekraft von Daten mit intrinsischem Personenbezug

Daten mit intrinsischem Personenbezug weisen, wie oben beschrieben, andere Charakteristika bei den kodierten Informationen auf, so dass die Bewertung eine andere Herangehensweise verlangt. In die gerichtliche Bewertung der Informationen muss dennoch immer mit einfließen, dass die Daten auf dem informationstechnischen System platziert oder von anderen Systemen aus zum ODS-Kontrollzentrum als vermeintliche Funde gesendet worden sein könnten. Beides kann — weil es extrinsische Aspekte sind — nicht glaubhaft widerlegt werden. Der Beweiswert derartig erlangter Daten muss im Lichte der obigen Erkenntnisse und im Vergleich zu forensischen Vorgehensweisen grundsätzlich zumindest als fragwürdig angesehen werden.

[329] Anderson, *Security Engineering*, 2008, Seite 147 ff.
[330] Chaos Computer Club, *Report 42*, 26.10.2011.
[331] Freiling, *Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, 27.9.2007, Seite 6.
[332] Fox, *Stellungnahme zur „Online-Durchsuchung", Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, 29.9.2007, Seite 15 oder auch Borchers und Kuri, *Kriminalbeamte fordern Verstärkung am digitalen Tatort*, 27.10.2011.

Es sei jedoch darauf hingewiesen, dass den erlangten Daten trotz des zuvor analysierten fehlenden Beweiswertes dennoch ein Erkenntniswert zufällt. Daher kann eine Online-Durchsuchung für andere Zwecke als die Strafverfolgung ein geeignetes Instrument sein.[333]

4.2.6 Fernsteuerung der ODS

Bei korrekter Implementation der kryptographischen Funktionen wäre eine Fernsteuerung der ODS für Dritte von außen verhinderbar, indem die Befehle von der ausforschenden Stelle mit asymmetrischer Verschlüsselung versehen gesendet würden. Die ODS würde nur auf Befehle reagieren, die vom privaten Schlüssel der Behörde signiert wurden. Die privaten Schlüssel der Behörde müssten dafür auch gegen Missbrauch gesichert werden, dies sprengte jedoch den Rahmen dieser Arbeit. Werden mindere Verschlüsselungsverfahren genutzt, steigt das Fernsteuerrisiko stark an.[334] Vom infiltrierten System aus könnten man die ODS jedoch auch so modifizieren, dass sie danach die Schlüssel Dritter akzeptieren würde.

4.3 Zusammenfassung der technisch-konzeptionellen und gesellschaftlichen Folgen

Die Analyse der technisch-konzeptionellen und gesellschaftlichen Folgen der Online-Durchsuchung ergab zunächst, dass informationstechnische Systeme in vielen Bereichen des menschlichen Lebens Einzug gehalten haben und dadurch den Alltag immer mehr zu Prozessen informationstechnischer Verarbeitung werden lassen. Dies gilt auch für die Erledigung von Staatsaufgaben, z. B. die Ausübung von Exekutivbefugnissen. Da die Befugnisse rechtlich geregelt sind, sollte sich die Beschränkung staatlicher Macht auch in informationstechnischen Werkzeugen wiederfinden.
Weiter ergab die Analyse, dass die Konvergenz verschiedener Lebensbereiche der Menschen im Computer ein immer größeres Ausmaß annimmt, ohne dass das Verständnis des Computers und seiner Funktionsweise vergleichbar mitwüchse. Dies ergibt eine Abhängigkeit des Einzelnen von Systemen, die er nicht überblickt. Beispiele sind unabsichtlich erzeugte Daten, die im Hintergrund Verhalten und Persönlichkeit des Nutzers zeitlich festhalten oder auch die zentrale Anhäufung von geronnener Telekommunikation in derartigen Systemen. All dies erreicht eine neue Qualität in der Ausweitung des Kernbereichs privater Lebensgestaltung ins Digitale.
Angewendet auf den Fokus der Arbeit ergab sich daraus, welche Eingriffstiefe eine Maßnahme wie die Online-Durchsuchung für den einzelnen Grundrechtsträger haben kann und regelmäßig haben würde. Die umfassenden Möglichkeiten und Funktionalitäten der ODS auf dem infiltrierten System lassen sich effektiv weder hinreichend einschränken, noch ist diese Beschränkung im Nachhinein belegbar.
Weiter ergab die Analyse, dass der Kernbereichsschutz einer solchen Maßnahme nicht technisch realisierbar ist und dadurch bei den durchführenden Behörden eine Anhäufung privater und privatester Daten stattfinden wird. Dies birgt auch ein erhöhtes Missbrauchspotenzial.
Auf den konkreten Nutzen der durch eine Online-Durchsuchung erlangten Informationen bezogen ergab sich, dass die Funde einer ODS forensischen Standards keinesfalls genügen. Daten-

[333] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 223.
[334] Chaos Computer Club, *Report 23*, 8.10.2011.

manipulation ist prinzipiell nicht erkennbar und Echtheit nicht technisch belegbar. Einzig die Unterscheidung in Daten mit intrinsischer und Daten mit extrinsischer Personenbeziehbarkeit deckte einen potenziell ermittlungsrelevanten Wert für Daten mit intrisischen Informationen für einen Personenbezug (Video-/Audiodaten mit Abbildcharakter) auf.

Nun sollen die bislang erlangten Erkenntnisse in konkrete Beziehung zum Urteil des Bundesverfassungsgerichtes zur Online-Durchsuchung gesetzt werden. Zunächst folgt jedoch eine knappe Zusammenfassung des Urteils unter den in der vorliegenden Arbeit angesprochenen Gesichtspunkten.

5 Das Bundesverfassungsgerichtsurteil: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Mit dem Urteil zur Online-Durchsuchung hat das Bundesverfassungsgericht informationstechnische Systeme grundsätzlich in den herrschenden Lebensgewohnheiten des modernen Bürgers verortet, indem es das *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* aus dem allgemeinen Persönlichkeitsrecht[335] ableitete.

5.1 Die Urteilsherleitung

Die Richter begründeten das neue Grundrecht mit der allgegenwärtigen Nutzung informationstechnischer Systeme[336] und deren Erlangung einer vorher unabsehbaren Bedeutung für die persönliche Entfaltung des Einzelnen.[337] Derartige Systeme werden nicht nur zunehmend für persönliche Aufzeichnungen[338] oder private Film- und Tondokumente[339] verwendet, sondern durch Vernetzung über das Internet immer mehr zum Medium herkömmlicher und neuartiger Kommunikationsdienste.[340] Das Gericht betonte die immer weiter steigende Konzentration und Verlagerung individueller und sozialer Facetten einer Person in technische Systeme, deren Komplexität mittlerweile so hoch ist, dass fremde Eingriffe teilweise weder wahrgenommen noch (für den durchschnittlichen Nutzer) technisch verhindert werden können.[341]
Ein heimlicher Eingriff in dieses System, so die Richter weiter, hat beim Betroffenen einen vollständigen Kontrollverlust über den Kernbereich seiner privater Lebensgestaltung zur Folge.[342] Da ein derartiger Eingriff weder direkten Raumbezug noch grundsätzliche Telekommunikationsfokusierung aufweist, aber andererseits nicht den Charakter einer einzelnen Datenerhebung hat, erkannte das Gericht eine Schutzlücke zwischen der Unverletzlichkeit der Wohnung, dem Brief-, Post- und Fernmeldegeheimnis und der informationellen Selbstbestimmung. Die

[335] Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.
[336] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 171.
[337] A.a.O. Absatz 170.
[338] A.a.O. Absatz 231.
[339] A.a.O. Absatz 272.
[340] A.a.O. Absatz 176.
[341] A.a.O. Absatz 180.
[342] A.a.O. Absatz 275.

Schutzlücke sahen die Richter im informationstechnischen System an sich, auf dessen Vertraulichkeit und Integrität der Einzelne für seine ungehinderte Persönlichkeitsentfaltung sogar angewiesen ist.[343]
Durch diese Abhängigkeit und die damit in einem freiheitlichen Rechtsstaat verbundenen berechtigten Erwartungen[344] von Vertraulichkeit und Integrität informationstechnischer Systeme ergibt sich nicht nur ein Recht auf die genannten Eigenschaften, sondern ein Grundrecht auf die Gewährleistung derselben,[345] auch gegenüber Dritten.[346] Es ist ein von der konkreten Sicherheit eines Systems unabhängiger Schutz der Vertraulichkeits- und Integritätserwartung[347] des Einzelnen an das System.
Um in ein derartiges Grundrecht heimlich für gefahrenabwehrende Zwecke eingreifen zu dürfen,[348] so das Gericht, müssen tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen,[349] doch es merkt explizit an, dass eine gesetzliche Maßgabe für diesen Eingriffsanlass möglicherweise gar nicht möglich ist.[350]
Auch zu Strafverfolgungszwecken kann ein Eingriff in das Grundrecht gerechtfertigt sein,[351] darauf wird jedoch wegen des gefahrenabwehrenden Charakters der beanstandeten Normen nicht weiter eingegangen.
Ist durch technische Vorkehrungen und rechtliche Vorgaben jedoch sichergestellt, dass durch einen Eingriff ausschließlich Daten eines laufenden Telekommunikationsvorgangs gewonnen werden können, ist das Brief-, Post- und Fernmeldegeheimnis der alleinige grundrechtliche Maßstab dafür.[352]
Zum Beweiswert der Erkenntnisse eines heimlichen Zugriffs auf informationstechnische Systeme äußert sich das Gericht nur hinsichtlich der angegriffenen Präventivnormen. Deren Ziel war nicht die Gewinnung revisionsfester Beweise, sondern die Erlangung von Kenntnissen zur Prävention im Vorfeld konkreter Gefahren.[353] Dafür sind die Erkenntnisse, so die Richter, trotz möglicherweise begrenztem Beweiswert geeignet.

5.2 Bewertung des Urteils

Das Bemerkenswerte des Urteils ist die Gewährleistung des Schutzes von informationstechnischen Systemen. Nicht nur die Daten des Systems, die nicht einmal persönlicher Natur sein müssen, werden geschützt, sondern das System an sich. Im Fokus liegt nicht die eigentliche Aktivität eines Eindringlings, sondern der Kontrollverlust durch das Eindringen selbst. Die staatliche Achtung solcher Systemgrenzen als Grenzen einer — zu körperlicher und räumlicher Ausdehnung orthogonalen — informationstechnischen Manifestation und Ausprägung einer

[343] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 200.
[344] A.a.O. Absatz 181.
[345] A.a.O. Absatz 204.
[346] A.a.O. Absatz 169.
[347] A.a.O. Absatz 206.
[348] A.a.O. Absatz 253.
[349] A.a.O. Absatz 247.
[350] A.a.O. Absatz 256.
[351] A.a.O. Absatz 207.
[352] A.a.O. Absatz 190.
[353] A.a.O. Absatz 223.

Person in ihrer Qualität als Persönlichkeit ist die eigentliche Aussage des Urteils. Eine absichtliche, heimliche Verletzung der Integrität des Systems ist folglich eine absichtliche, heimliche Verletzung der Integrität der Person und somit „eine sukzessive Einschränkung und schließlich Auflösung dessen, was wir als Grundwert des Schutzes der Person, ihrer Autonomie, Freiheit und Würde kennen“.[354]

Oder anders ausgedrückt: Nicht, dass Dritte mein Tagebuch lesen oder meine Selbstgespräche mithören, ist die Integritätsverletzung, sondern die Tatsache, dass sie es jederzeit im Geheimen tun können, aber ich mich nicht wehren kann. Nicht erst der konkrete Akt ist die Bedrohung, sondern dessen Möglichkeit.

Hier offenbart sich die Ableitung aus dem allgemeinen Persönlichkeitsrecht, denn „im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Ihrem Schutz dient [...] das [...] allgemeine Persönlichkeitsrecht, das gerade auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen der menschlichen Persönlichkeit Bedeutung gewinnen kann“.[355]

Auch hat das Gericht die Streubreite der Maßnahme erkannt, die sowohl in der Ansammlung persönlichster Informationen verschiedener Personen in einem informationstechnischen System, als auch in der zeitlichen Dimension eines längeren Eingriffs begründet sind.[356]

Erwähnung haben auch die weiter oben „Schattendaten“ genannten Metadaten und Logs gefunden, die nicht explizit durch den Benutzer angelegt werden, sondern schon durch die Nutzung des informationstechnischen Systems entstehen und auch ausgewertet werden können.[357]

Durch den meist automatisierten Prozess des Datensammelns durch Online-Durchsuchungen sah sich das Gericht gezwungen, kein Erhebungsverbot bezüglich des Kernbereichs privater Lebensgestaltung auszusprechen, sondern verlagerte den Kernbereichsschutz effektiv[358] in eine eigens dafür geschaffene Durchsichtphase.[359] Gründe für die Aufweichung sind in der Universalität der informationstechnischen Systeme zu suchen. So geben sie den Einen Werkzeuge an die Hand, effektiven kryptographischen Selbstschutz zu betreiben, den Nächsten Mittel zum Verüben von Straftaten und wieder Anderen einen digitalen Kernbereich ungeahnter Intensität und — zukünftig — ungeahnten Ausmaßes. Weil eine Trennung dieser Nutzungsaspekte weder generell zu erwarten noch im Vorhinein einer Maßnahme möglich ist, muss eine Entscheidung getroffen werden, mit wie viel Eingriff in das Eine (z . B. Straftatmittel) die Gesellschaft für den Eingriff in das Andere (umfassende Persönlichkeitsausforschung) bereit ist zu „zahlen“. Die hohen Schranken sind an dieser Stelle das verfassungsrechtliche Mittel für die Manifestation der Entscheidung. Zu beachten ist hier, wie informationstechnische Gegebenheiten gesellschaftlich-rechtliche Handlungswege vorgeben.

---

[354] Pfitzmann, *Rede vor dem Bundesverfassungsgericht als Sachverständiger zur Online-Durchsuchung*, 10.10.2007, Seite 4.

[355] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Volkszählung*, 15.12.1983, Abschnitt C II 1a.

[356] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 233 und 235.

[357] A.a.O. Absatz 178.

[358] Siehe Unterabschnitt 4.1.4 (Technischer Kernbereichsschutz).

[359] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 280.

Die vorliegende Arbeit könnte Schranken, legitimen Zweck, Geeignetheit, Erforderlichkeit und Angemessenheit einer rein rechtlichen Maßnahme nicht bewerten. Weil die Online-Durchsuchung jedoch immer einer technischen Umsetzung bedarf und diese Umsetzung sogar zentrales Element der Maßnahme ist, müssen die technischen Möglichkeiten und Grenzen des Instruments ein Hauptbetrachtungsgegenstand der Verhältnismäßigkeitsüberlegungen sein.
Nach den Untersuchungen in Abschnitt 3 (Die Online-Durchsuchung en detail) und Abschnitt 4 (Technisch-konzeptionelle und gesellschaftliche Folgen der Online-Durchsuchung) können die rechtlichen Verhältnismäßigkeitsüberlegungen und die daraus entwickelten Anforderungen des Bundesverfassungsgerichtes mit den technischen Gegebenheiten zusammengebracht und reflektiert sowie die tatsächlichen rechtlichen Konsequenzen herausgearbeitet werden.

5.2.1 Antworten auf die technischen Forderungen des Gerichts

Wie weiter oben erwähnt, müssen legitimer Zweck, Geeignetheit, Erforderlichkeit und Angemessenheit einer verfassungsgemäßen Maßnahme zugrunde liegen. Der Maßnahme des heimlichen Zugriffs auf informationstechnische Systeme zur Gefahrenabwehr sprach das Bundesverfassungsgericht die Möglichkeit des legitimen Zwecks, der Geeignetheit, der Erforderlichkeit und der Angemessenheit nicht grundsätzlich ab, stellte aber bei der angegriffenen Norm einen Verstoß gegen die Angemessenheitsforderung fest.[360]
Außer der Legitimität haben alle Aspekte der Maßnahme eine explizite informationstechnische Dimension: die konkrete technische Umsetzung. Deshalb ist es im Rahmen dieser Arbeit möglich und zulässig, die Angemessenheitsüberlegungen des Gerichts zu hinterfragen.
Zwar setzte das Gericht die Schranken für einen verfassungsmäßigen Einsatz eher hoch, doch die oben belegten rechtsstaatlich weder begrenzbaren noch kontrollierbaren immensen Fähigkeiten einer heimlichen Online-Durchsuchung ließen in Verbindung mit dem ursprünglich absolut geschützten, aber technisch nicht schützbaren Kernbereich privater Lebensführung eigentlich eine prinzipielle Verfassungswidrigkeit vermuten. Heimliche Maßnahmen mit derartiger Streubreite, Eingriffstiefe und Missbrauchspotenzial, bei denen selbst im entdeckten Schadensfall nicht einmal eine Person zur Verantwortung gezogen werden könnte, werfen grundlegende Fragen über die Grenzen rechtsstaatlichen Handelns auf.
Da mit offenen Durchsuchungen „regelmäßig dieselben Erkenntnisse gewonnen werden können“,[361] muss schon die Erforderlichkeit der Maßnahme teilweise in Frage gestellt werden, und speziell für die Strafverfolgung gilt, dass der grundsätzlich fehlende Beweiswert erlangter Daten die Geeignetheitsforderung ins Leere laufen lässt.

Mit Blick auf die in Aussicht gestellte, niedrigere Eingriffsschwelle für eine Quellen-TKÜ im Gegensatz zur Online-Durchsuchung muss festgehalten werden, dass der Wunsch der Trennung der beiden Maßnahmen nach Erkenntnisorientierung und Eingriffstiefe verfahrensrechtlich sicher verständlich, aber technisch grundsätzlich nicht abbildbar ist. Daher sind jegliche heimlichen Eingriffe in informationstechnische Systeme nur unter Beachtung der vollen Eingriffsschranke für eine Online-Durchsuchung verfassungskonform durchführbar, regelmäßig unter zusätzlicher Einbeziehung der Schranke für Telekommunikationsüberwachungen,

[360] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 218 ff.
[361] Bundesregierung der 16. Wahlperiode, *Drucksache 16/3973*, 28.12.2006, Antwort zu Frage 10.

denn wie in Unterabschnitt 3.2 (Die Unterscheidung von Quellen-TKÜ und Online-Durchsuchung) und weitergehend in Unterabschnitt 4.1.1 (Wohnraumüberwachung, Telekommunikationsüberwachung, Quellen-TKÜ und die Online-Durchsuchung) gezeigt wurde, ist eine klare Trennung von Daten in Telekommunikationsdaten und Nichttelekommunikationsdaten in heutigen hochvernetzten Systemen weder konzeptionell möglich noch technisch machbar. Die Grauzone ist zu groß und Daten können technisch bedingt nicht so sicher unterschieden werden, wie es nötig wäre, um geringere Schranken für einzelne Zielrichtungen in Erwägung zu ziehen.

Wie in Unterabschnitt 4.2.2 (Zuordnung zu Personen) ausgeführt wurde, ist allerdings eine andere Unterscheidung von Daten sinnvoll. Die Analyse der Personenzuordenbarkeit von Daten resultierte in zwei Aspekten: Daten können extrinsisch personenbeziehbar oder intrinsisch personenbezogen sein.

Daten mit intrinsischem Personenbezug sind für strafverfolgende und gefahrenabwehrende Zwecke vermutlich sinnvoll verwertbar. Somit wären Eingriffsbefugnisse nach Maßgabe und Schranken des Bundesverfassungsgerichts denkbar.

Daten mit extrinsischer Personenbeziehbarkeit sind jedoch aufgrund ihres sehr geringen Beweiswertes für strafverfolgende Zwecke ungeeignet, Eingriffsbefugnisse in dieser Hinsicht wären absolut unverhältnismäßig. Für gefahrenabwehrende Zwecke gilt jedoch „nicht, dass den erhobenen Daten kein Informationswert zukommt“,[362] daher wäre eine Online-Durchsuchung nach Maßgabe und Schranken des Bundesverfassungsgerichts im Vorfeld konkreter Gefahren denkbar.

Dennoch muss immer beachtet werden, dass das Gericht keine Empfehlungen für notwendige oder sinnvolle Eingriffsbefugnisse ausspricht, sondern nur verfassungsmäßige Schranken für eventuelle Ermächtigungen festlegt. Sollte sich die Gesellschaft nach ausführlicher Diskussion entscheiden, dieses Instrument generell nicht im Einsatz sehen zu wollen, kann und muss eine Schaffung von Ermächtigungen unterbleiben bzw. rückgängig gemacht werden.
Dass die Online-Durchsuchung technisch-konzeptionell auf diese Weise möglich und verfassungsmäßig wäre, ist daher allein kein Anlass für die Schaffung von Ermächtigungen.

5.2.2 Technischer sowie verfassungsrechtlicher Aufklärungsbedarf

Schwer zu erklären ist jedoch der immer noch mangelnde Respekt der Exekutivorgane gegenüber der informationstechnischen Ausprägung der Person. Konnte man vor dem Urteil zur Online-Durchsuchung bei Bestrebungen wie dem für ungültig erklärten Verfassungsschutzgesetz[363] wohlwollend immer noch eine gewisse „digitale Jungfräulichkeit“ annehmen, die hätte erklären können, dass für die damals geplanten Eingriffe kein Richtervorbehalt vorgese-

[362] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 223.
[363] § 5 Abs. 2 Nr. 11, VSG NRW, eingefügt/geändert durch das Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20.12.2006.

hen war,[364] weitgehende Ausnahmen von der grundrechtlich gebotenen Benachrichtigungspflicht eingeräumt wurden[365] sowie die Erkenntnisse an jegliche Behörde in Deutschland, ausländische öffentliche Stellen oder sogar über- und zwischenstaatliche Stellen[366] hätten übermittelt werden können, so wird bis zum heutigen Tage der doch recht klare Richterspruch prominent fehlgedeutet[367] und gar bewusst missachtet.[368] Obwohl diese Arbeit ihre Stärke in konzeptionell-informationstechnischen Überlegungen sieht, sei ein praktischer Einlass zu Illustrationszwecken erlaubt:

Weil bestimmte Tatsachen die Annahme rechtfertigten, die vom BKA eingesetzte Quellen-TKÜ-Software beinhalte eine Nachladefunktion für beliebigen Code,[369] äußerte der Präsident des BKA, Jörg Ziercke, am 19.10.11 im Innenausschuss, „gegen eine bloße Aktualisierungsfunktion kann das BVerfG keine Einwände haben, weil sonst die Maßnahme an sich gefährdet wäre."[370]

Abgesehen davon, dass diese Aussage eine fragwürdige Denkweise gegenüber der Rolle des Bundesverfassungsgerichtes offenbart, ist dies ein Zugeständnis, dass keine technische Beschränkung der Software auf Telekommunikationsdaten vorgenommen worden ist, denn mit einer Aktualisierung ist jede beliebige Funktion realisierbar, und keine davon ist protokollierbar.[371]

Neben anderen Fällen und Aussagen[372] zeigen diese Beispiele, dass das Urteil zur Online-Durchsuchung noch nicht gänzlich verstanden oder akzeptiert wurde. Insbesondere die Leitidee des Urteils, dass es nicht um konkret ausgeübte Kontrolle, sondern andersherum um den Kontrollverlust des Betroffenen geht, muss begriffen werden. So müssen sich die technischen Vorgaben im Nichtvorhandensein unzulässiger Funktionalität äußern, nicht im Nichteinsatz unzulässiger, aber vorhandener Funktionalität. In Anbetracht des in Abschnitt 4 (Technisch-konzeptionelle und gesellschaftliche Folgen der Online-Durchsuchung) beschriebenen Grundverständnisses staatlicher Handlungsprinzipien ist an dieser Stelle noch viel Aufklärungsarbeit zu leisten.

Man kann damit schließen, dass das Gericht die technischen, individuellen und gesellschaftlichen Gefahren der Maßnahme erfreulich klar erkannt hat. Doch trotz der formulierten hohen Schranken für Eingriffsermächtigungen in das neue Grundrecht bleibt die grundsätzliche Zulässigkeit angesichts des Prinzips des absolut geschützten Kernbereichs zumindest strittig. Eine konkrete verfassungsmäßige Ausgestaltung[373] der Gesetzeslandschaft durch die Legislative steht jedoch genauso aus wie die Einhaltung der aktuell gültigen Normen durch die Exekutive.

[364] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung*, 27.2.2008, Absatz 122.

[365] A.a.O. Absatz 123.

[366] A.a.O. Absatz 128.

[367] Hoffmann und Tomik, *„Es gibt keine rechtliche Grauzone"*, 15.10.2011.

[368] Trotz des Beschlusses der Rechtswidrigkeit der Bildschirmfoto-Quellen-TKÜ am 20.01.2011 (Az: 4 Qs 346/10 LG Landshut) wurde die Maßnahme weiter eingesetzt Bayerisches Staatsministerium der Justiz und für Verbraucherschutz, *Drucksache 16/8125*, 29.04.2011.

[369] Chaos Computer Club, *Report 42*, 26.10.2011.

[370] Ziercke, *Sprechzettel für die Teilnahme des Präsidenten des Bundeskriminalamtes Jörg Ziercke an der 53. Sitzung des Innenausschusses zu TOP 24a (24b, 24c)*, 19.10.2011, Seite 10.

[371] Siehe Unterabschnitt 3.1.5 (Update der Software) und Abschnitt 3.3 (Fehlende Protokollierbarkeit).

[372] Z. B. afp (Agence France-Presse), *Baden-Württemberg stoppt den Trojaner-Einsatz*, 10.10.2011.

[373] Vergleiche diesbezügliche Vorschläge in Sieber, *Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen*, 9.10.2007, Seite 19.

Dies ist ein beunruhigender Zustand für einen Rechtsstaat.

Auch wenn die Auslotung der Möglichkeiten und Grenzen einer staatlichen Nutzung informationstechnischer Instrumente im Ergebnis den Verzicht bestimmter Anwendungsszenarien bedeutet, ist dieser notwendig und richtig, um dem Grundgesetz und der verfassungsmäßigen Ordnung Genüge zu tun.

6 Schluss

6.1 Fazit und offene Probleme

In der rechtlichen Begrifflichkeit sind informationstechnische Systeme das, was sie in der Lebenswirklichkeit vieler Menschen bereits sind: keine lose Ansammlung verschiedener Geräte, davon unabhängiger Verbindungen zu Netzspeichern oder einzelner Webmailinterfaces, sondern eine zusammenhängende logische Einheit, die man vielfältig verwendet und auf die man von mehreren Stellen aus zugreifen kann. Auf diese Art verwenden es die Nutzer auch und haben dementsprechende Erwartungen an *ihr* System. Ob während des Schreibens einer E-Mail im Webinterface Daten zwischen dem Server und dem Browser ausgetauscht werden oder nicht und ob das schon einen Kommunikationsvorgang darstellt, ist eine technische Sicht und dem Nutzer unwichtig, für ihn ist es das Schreiben einer E-Mail mit seinem *informationstechnischen System*.

Auch wenn es aktuell noch Teile dieses System gibt, die noch nicht lückenlos verbunden sind (z. B. Multimediasystem und Auktionsplattformen), ist die Tendenz zur Zentralisierung (z. B. Datensynchronisationskonzepte über mehrere physische Geräte hinweg) klar erkennbar, wobei die eigentliche Komplexität dadurch weiter steigt. Somit steigt auch die zu schützende Oberfläche, die nun in ihrer Integrität und inneren Vertraulichkeit zumindest rechtlich gewährleistet wird.

Doch es gibt noch viele praktische Probleme zu lösen, die teilweise ihren Ursprung in konzeptionellen Gründen, aber auch in ganz praktischen Umständen haben.

Diese Fragen umfassen: Wie kann damit umgegangen werden, wenn z. B. eine ODS auf dem System des Betroffenen aktiv ist und aus technischen Gründen nicht beendet werden kann, obwohl die Maßnahme „Online-Durchsuchung“ rechtlich hätte abgeschlossen werden sollen. Weiter müsste diskutiert und geregelt werden, ob generell nur die direkte Aufbringung zulässig sein sollte, um Kollateralschäden abzumildern. In bestimmten Fällen könnte auch nur die Analyse der Abstrahlungen erlaubt werden, um die Eingriffstiefe zu verringern und die Integrität des Systems zu bewahren.

Zusätzlich muss die technische Qualität einer solchen Software zukünftig streng kontrolliert und reglementiert werden, denn die aktuell bekannt gewordenen ODS-Implementationen[374] weisen derartig gravierende technische Defizite auf, dass man sich nicht vorstellen möchte, dass ein Rechtsstaat sich mit einem solchen Instrument behutsam zwischen den unantastbaren Kernbereichen seiner Bürger bewegen will.

[374] Siehe Chaos Computer Club, *Report 23*, 8.10.2011 und Chaos Computer Club, *Report 42*, 26.10.2011.

Sollte diese Aufgabe an Dritte weitergegeben werden, weil das Bundesministerium des Innern möglicherweise nicht grundlegend über genügend Sachverstand verfügt, sind strenge Regeln für die Zusammenarbeit vorzusehen. In diesem Kontext muss der Schutz der Bürger über den Geschäftsinteressen des potenziellen Partnerunternehmens stehen. Eine Nichtaushändigung des Quellcodes ist nicht akzeptabel. Die bislang eingesetzten „Positivtests" zur „Kontrolle" der tatsächlichen Funktionen der ODS-Implementation[375] lassen keine Prüfung auf Verfassungskonformität zu und entbehren darüber hinaus jeglicher Professionalität. Extern eingekaufte Software muss demnach immer im Quellcode vorliegen, um auch daraufhin überprüft zu werden, dass keine anderen Funktionen verborgen oder indirekt möglich sind, auch wenn dies prinzipiell nicht abschließend machbar ist.[376] Es besteht also Qualitätskontroll- und Regelungsbedarf.[377]

Auch die gesetzlichen Regelungen für beschlagnahmte Datenträger und Rechnersysteme sollte in Anbetracht des Urteils überdacht werden. Insbesondere die sogenannte „Online-Durchsuchung light" nach § 110 Abs. 3 StPO[378] (die „Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen darf auch auf hiervon räumlich getrennte Speichermedien [...] erstreckt werden")[379] muss einer erneuten Prüfung unterzogen werden bzw. die technische Gegebenheiten mit einbeziehenden Reformvorschläge müssen umgesetzt werden.[380]

Die Forderung muss also lauten: Der Staat sollte nicht nur mit dem technischen Fortschritt der Kriminellen mithalten wollen, sondern zuvorderst und mit allem Nachdruck mit der steigenden Bedrohung seiner Bürger durch den technischen Fortschritt. Dass der Begriff des unantastbaren Kernbereichs privater Lebensgestaltung in seiner jetzigen Form dafür das richtige Mittel ist, wird immer unwahrscheinlicher, da er in der Vergangenheit nicht einmal in der analogen Welt schlagkräftig verwendet wurde.[381]

6.2 Zusammenfassung

Diese Arbeit beschäftigte sich mit der heimlichen Online-Durchsuchung, einer staatlichen Maßnahme zur Informationsgewinnung durch den heimlichen Zugriff auf informationstechnische Systeme. Diese heftig umstrittene Maßnahme wurde und wird nach wie vor eingesetzt. Zunächst wurde der historische Kontext und die generelle politische Diskussion umrissen, woraufhin Methodik und Grundbegriffe geklärt wurden.

Die Methodik bestand darin, aus Aussagen über die gewünschten Fähigkeiten einer heimlichen Online-Durchsuchung die konzeptionellen Anforderungen an eine ODS zu erstellen, die-

[375] Ziercke, *Sprechzettel für die Teilnahme des Präsidenten des Bundeskriminalamtes Jörg Ziercke an der 53. Sitzung des Innenausschusses zu TOP 24a (24b, 24c)*, 19.10.2011, Seite 12.

[376] Thompson, „Reflections on Trusting Trust", Aug. 1984.

[377] Weitere gute Vorschläge sind bei Hansen und Pfitzmann, „Techniken der Online-Durchsuchung", 2008, Seite 152-154 zu finden.

[378] Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 5 des Gesetzes vom 23. Juni 2011 (BGBl. I S. 1266) geändert worden ist.

[379] Siehe dazu Kurz und Buermeyer, *Vortrag: Das Grundrecht auf digitale Intimsphäre*, 27.12.2008.

[380] Sentker (Die ZEIT) und Blumenthal, *Diskussion: Vertraue niemandem – Mit Sicherheit im Netz*, 12.12.2008.

[381] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum Tagebuchinhalt I*, 14.9.1989, Absatz 30 und neuer: Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum Tagebuchinhalt II*, 1.2.2006, Absatz 7.

se dann unter Beachtung der modernen Rechnerarchitektur zu analysieren und erwachsende Folgen sowie deren gesellschaftliche Konsequenzen daraus zu entwickeln. Im Wesentlichen hat sich die angewandte Methodik bewährt, dabei wurden wenige Rückgriffe auf konkrete Implementationsfragen getan, um den prinzipiell-konzeptionellen Anspruch der Arbeit zu gewährleisten. Die Ergebnisse sind reichhaltig und umreißen das, was mit moderner Rechnerarchitektur in dieser Hinsicht überhaupt möglich ist. Danach wurde das Bundesverfassungsgerichtsurteil zur Online-Durchsuchung zusammengefasst und die entwickelten technischen Eigenschaften und Folgen einer Online-Durchsuchung darauf angewendet. Die Arbeit endet mit einer kurzen Kritik der derzeitigen Praxis und noch offenen Problemen.

Im Ergebnis zeigt sich, dass eine Online-Durchsuchung und deren technische Umsetzung prinzipiell folgende Merkmale aufweist:

1. Eine Funktionsbeschränkung der Software kann weder sichergestellt noch belegt werden, daher muss immer die maximale Eingriffshürde zur Anwendung kommen.

2. Erlangte Daten haben grundsätzlich keinen Beweiswert, sofern sie keinen eigenen intrinsischen Personenbezug aufweisen (z. B. Bilder, die Personen zeigen).

3. Die Trennung von Telekommunikations- und Nichttelekommunikationsdaten ist technisch nicht hinreichend lösbar, daher muss immer die maximale Eingriffshürde zur Anwendung kommen.

4. Der Kernbereich privater Lebensgestaltung ist praktisch immer betroffen, technischer Kernbereichsschutz ist nicht möglich.

Diese Leitsätze und die dorthin führenden Argumentationen sowie aufgezeigten Risiken können und sollen dazu beitragen, die andauernde Diskussion über das Instrument „Online-Durchsuchung“ sachlich zu unterfüttern. Denn wie auch immer das Resultat dieser gesellschaftlich wichtigen Debatte aussehen mag, sie sollte bei einem so komplexen und neuen Gebiet wie der Informationstechnik nicht ideologisch geführt werden.

6.3 Schlusswort

Daten auf informationstechnischen Systemen sind weder sinnlich wahrnehmbar noch sind die Systeme selbst für die Nutzer hinreichend begreifbar. Das einzige, was die Verlagerung täglicher, höchstpersönlicher Angelegenheiten in derartige Systeme tragen kann, ist Vertrauen. Vertrauen in Computer, Vertrauen in Kryptographie, Vertrauen in Mitmenschen, Vertrauen in Netze, Vertrauen in Unternehmen und auch Vertrauen in den Staat, dass nichts in dieser Kette dem Einzelnen schaden kann oder zumindest schaden will. Nichts in dieser Aufzählung ist auch nur halbwegs überprüfbar oder beherrschbar für einzelne Personen, deshalb ist die Informationsgesellschaft auch immer eine Vertrauensgesellschaft.[382] Hier handelt es sich jedoch nicht um das Vertrauen in einen langjährigen Freund oder andere Beziehungen zur Person, in der sich das Vertrauen aufbauen konnte, sondern um ein Vertrauen in Dinge, das diese nur

[382] Siehe generell Klumpp, *Informationelles Vertrauen in der Informationsgesellschaft*, 2008.

dadurch erhalten, dass viele andere Menschen ihnen auch vertrauen. Weil dadurch permanent mit Komplexität umgegangen wird, die fast nicht mehr zu durchdringen ist, werden Kompensationsmechanismen immer wichtiger. Konzepte wie die Bewertung von Online-Verkäufern, die Zertifizierung von Handelspartnern oder generelle Markenbildung werden dabei immer wichtiger, um zumindest die Risikoempfindung abzumildern und so das Vertrauen in komplexe informationstechnische Medien zu erhalten.

Wenn der Staat sich dem Einzelnen und seiner Techniknutzung nicht entgegenstellen will, muss er Vertrauen in Computer und Netze schaffen.[383] Tut er das nicht mit aller Kraft oder unglaubwürdig, vergibt er eine Chance, in der zukünftigen vernetzen Welt das Primat der Politik zu behaupten, und riskiert so einen grundsätzlichen Legitimationsverlust.

Ein Weg, das Vertrauen zu verspielen, sind Staatsorgane, die z. B. einerseits über Wirtschaftsspionage und Such-Trojaner aufklären,[384] gleichzeitig aber Online-Durchsuchungen durchführen. Ob bei den Aufklärungsveranstaltungen Informationen zurückgehalten werden oder gezielte Falschinformationen verbreitet werden, muss sich der Bürger da fragen und zweifelt zu Recht. Auch wenn das Bundesamt für Sicherheit in der Informationstechnik „nicht beauftragt (ist), technische Möglichkeiten zur Durchführung von Online-Durchsuchungen zu entwickeln“,[385] ist die Vorstellung doch eigenartig, dass die eine Behörde aktiv die Sicherheit der informationstechnischen Systeme des Landes verbessern soll, während eine zweite aktiv genau dagegen vorgeht. Dieser Interessenkonflikt sorgt schon jetzt für Verwirrung bei den Bürgern und wird auch in Zukunft ausgenutzt werden, Virenmails mit vermeintlicher Warnung vor dem Bundestrojaner sind schon zu beobachten.[386] Ein zweiter Weg, Vertrauen zu verspielen, sind einfache Forderungen nach mehr Vertrauen, wie es die Generalbundesanwältin Monika Harms im Jahre 2008 bezüglich der BKAG-Novellierung getan hat.[387] Insbesondere wenn sich später zeigt, dass es klare Rechtsübertretungen seitens der Staatsorgane bezüglich gleichartiger Regelungen gegeben hat, diese gerichtlich bestätigt wurden und politische Vertreter trotzdem noch auf ihrem erwiesenermaßen falschen Rechtsverständnis beharren.[388]

Eigentlich sollte der Staat dem Bürger vertrauen, während dieser wiederum den Staat kontrolliert. Wenn der Bürger schon vertrauen soll und muss, dann zuvorderst auf eine grundgesetzmäßige Ausgestaltung der rechtlichen Rahmenbedingungen durch die von ihm gewählten Vertreter sowie die ordnungsgemäße Anwendung dieser Regelungen durch die Exekutive.

Nach akustischer Wohnraumüberwachung, Verbindungsdatenurteil, Vorratsdatenspeicherung, Online-Durchsuchung und Quellen-TKÜ-Bildschirmfotos ist dieses Vertrauen allerdings nach wie vor stark beeinträchtigt. Vor allem die noch immer eminente Abwesenheit notwendigen

[383] Siehe Aufgaben des Bundesamtes für die Sicherheit in der Informationstechnik (BSI), Das Bundesamt für Sicherheit in der Informationstechnik, *Aufgaben des BSI*, 2011.
[384] Wilkens, *Verfassungsschutz klärt über Wirtschaftsspionage und Such-Trojaner auf*, 16.3.2007.
[385] Bundesregierung der 16. Wahlperiode, *Drucksache 16/4997*, 10.4.2007, Frage 9.
[386] Kleinz und Wilde, *Virenmail mit Verweis auf Bundestrojaner*, 5.5.2007.
[387] Borchers und Kuri, *Generalbundesanwältin fordert Vertrauen in Ermittlungsmaßnahmen*, 3.10.2008.
[388] Siehe Unterabschnitt 4.1.1 (Wohnraumüberwachung, Telekommunikationsüberwachung, Quellen-TKÜ und die Online-Durchsuchung).

Wissens über digitale Sachverhalte[389] sorgt dafür, dass sich oftmals diejenigen durchsetzen,[390] deren Arbeit Eingriffe in Grundrechte erfordert. Im Ergebnis ist es mehr als beängstigend, wenn sogar die neuen Verfassungsschützer Deutschlands — die Richter des Bundesverfassungsgerichtes — fast resignierend konstatieren:

> Inzwischen scheint man sich an den Gedanken gewöhnt zu haben, dass mit den mittlerweile entwickelten technischen Möglichkeiten auch deren grenzenloser Einsatz hinzunehmen ist. Wenn aber selbst die persönliche Intimsphäre [...] kein Tabu mehr ist, vor dem das Sicherheitsbedürfnis Halt zu machen hat, stellt sich auch verfassungsrechtlich die Frage, ob das Menschenbild, das eine solche Vorgehensweise erzeugt, noch einer freiheitlich-rechtsstaatlichen Demokratie entspricht.[391]

Letztendlich bleibt zu hoffen, dass die Vertreter des Volkes die Berichte und Ergebnisse ihrer eingesetzten Enquêtekommision „Internet und digitale Gesellschaft“ in Ruhe lesen, daraus lernen und sich auch generell mit dem Internet sowie dessen technischen Grundlagen auseinandersetzen. Doch wie so oft sind die eigentlichen Probleme nicht technischer Natur, denn solange ein Verfassungsminister nur „akzeptiert“, dass man zum Schutz der Grundrechte „auch mal auf eine Maßnahme verzichten muss“,[392] und sich nicht aktiv dafür einsetzt, ist noch viel politische Arbeit nötig.

[389] Es gibt auch Ausnahmen, siehe Kurz, „Die Geister die ich rief... Deine Spuren im Netz, Symposium 2007“, 2008, Seite 4.

[390] Siehe Kritik am BKAG-Entwurf und ihre Nichteinbeziehung in die Novellierung, Schaar, *Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Gesetzentwurf der Fraktionen der CDU/CSU und der SPD: Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, BT-Drs. 16/9588*, 15.9.2008, Geiger, *Stellungnahme zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt BT-Drucksache 16/9588*, August 2008. Die Konsequenz ist bekannt und wird bald verhandelt.

[391] Bundesverfassungsgericht, *Bundesverfassungsgerichtsurteil zum großen Lauschangriff*, 3.3.2004, Absatz 373.

[392] Hoffmann und Tomik, *„Es gibt keine rechtliche Grauzone“*, 15.10.2011.

7 Quellen

Literatur

Anderson, Ross: *Security Engineering, A Guide to Build Dependable Distributed Systems*, 2. Aufl., Indianapolis: Wiley, 2008.

Bäcker, Matthias: „Das IT-Grundrecht“, in: *Das neue Computergrundrecht*, hrsg. von Robert **Uerpmann-Wittzack**, LIT Verlag, 2009.

Bielefeldt, Heiner: *Freiheit und Sicherheit im demokratischen Rechtsstaat, Essay No. 1*, Berlin: Deutsches Institut für Menschenrechte, Dezember 2004.

Bogk (Chaos Computer Club), Andreas: *Antwort zum Fragenkatalog zur Verfassungsbeschwerde 1 BvR 370/07 und 1 BvR 95/07*, 23.9.2007.

Braun, Frank: „0zapftis – (Un)Zulässigkeit von “Staatstrojanern”“, in: *Kommunikation & Recht* 11 (2011), Passau, Seiten 681–686, URL: `http://www.kommunikationundrecht.de/delegate/resources/dok751.pdf?fileid=dok751.pdf_kur&type=asset`.

Buermeyer, Ulf: „Die Online-Durchsuchung. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme.“, in: *Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht (HRRS)* 4 (2007), Seiten 154–166, URL: `http://www.hrr-strafrecht.de/hrr/archiv/07-04/index.php?sz=8`.

Buermeyer, Ulf und Matthias **Bäcker**: „Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des §100a StPO“, in: *Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht (HRRS)* 10 (2009), Seiten 433–441, URL: `http://www.hrr-strafrecht.de/hrr/archiv/09-10/index.php?sz=8`.

Bundesamt für Sicherheit in der Informationstechnik: *Leitfaden „IT-Forensik“*, Version 1.0.1, Bonn, 2011.

Bundesministerium des Innern: *Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien*, Berlin, 22.8.2007.

Bundesministerium des Innern: *Fragenkatalog des Bundesministeriums der Justiz*, Berlin, 22.8.2007.

Bundesregierung der 16. Wahlperiode: *Drucksache 16/4803, Schriftliche Fragen mit den in der Woche vom 19. März 2007 eingegangenen Antworten der Bundesregierung*, 23.3.2007.

Bundesregierung der 16. Wahlperiode: *Drucksache 16/4997, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Sabine Leutheusser-Schnarrenberger, Jörg*

van Essen, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 16/4795 – Online-Durchsuchungen, 10.4.2007.

Bundesregierung der 16. Wahlperiode: *Drucksache 16/6535, Schriftliche Fragen mit den in der Woche vom 24. September 2007 eingegangenen Antworten der Bundesregierung*, 28.9.2007.

Bundesregierung der 16. Wahlperiode: *Drucksache 16/6885, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Dr. Max Stadler, Hartfrid Wolff (Rems-Murr), weiterer Abgeordneter und der Fraktion der FDP – Drucksache 16/6694 – Rechtsstaatliche Probleme bei der Überwachung der Telekommunikation über das Internet*, 30.10.2007.

Bundesregierung der 16. Wahlperiode: *Drucksache 16/3973, Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Petra Pau, Kersten Naumann und der Fraktion DIE LINKE. – Drucksache 16/3787 – Rechtmäßigkeit und Anwendung von Online-Durchsuchungen*, 28.12.2006.

Chaos Computer Club: *QUELLEN-TKÜ-Stellungnahme des Chaos Computer Clubs*, 2009.

Chaos Computer Club: *Report 23, Dem Chaos Computer Club (CCC) wurde Schadsoftware zugespielt, deren Besitzer begründeten Anlaß zu der Vermutung hatten, daß es sich möglicherweise um einen „Bundestrojaner" handeln könnte. Einen dieser Trojaner und dessen Funktionen beschreibt dieses Dokument, die anderen Versionen werden teilweise vergleichend hinzugezogen.*, Berlin, 8.10.2011.

Chaos Computer Club: *Report 42, Dem Chaos Computer Club (CCC) wurden weitere Exemplare der als Staatstrojaner bekanntgewordenen Schadsoftware zugespielt. Zwei Wochen nach der Veröffentlichung der Analyse des Trojaners aus dem Jahr 2008 möchten wir die bislang modernste bekannte Variante der wohl populärsten staatlichen Schnüffelsoftware des Landes näher vorstellen.*, Berlin, 26.10.2011.

Coy, Wolfgang: „Brauchen wir eine Theorie der Informatik?", in: *Informatik-Spektrum* 12:5 (1989).

Eck, Wim van: „Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?", in: *Computers & Security* 4 (1985), S. 269–286.

Enquêtekommision „Internet und digitale Gesellschaft": *Zweiter Zwischenbericht, Medienkompetenz*, 21.10.2011.

Fox, Dirk: *Stellungnahme zur „Online-Durchsuchung", Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, Version 1.1, 29.9.2007.

Freiling, Felix: *Schriftliche Stellungnahme zum Fragenkatalog Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07*, Mannheim, 27.9.2007.

Geiger, Hansjörg: *Stellungnahme zum Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt BT-Drucksache 16/9588*, August 2008.

Geschonneck, Alexander: *Computer-Forensik*, 5. Aufl., Heidelberg: dpunkt.verlag, 2011.

Goodman, Nelson: *Languages of Art, An Approach to a Theory of Symbols*, 2. Aufl., Gazelle Book Services, 1976.

Hansen, Markus und Christian **Krause**: *Heimliche Online-Durchsuchung – Wie geht's, wie schütze ich mich?, Folien des Vortrags auf der Sommerakademie 2007-08-27, Thema: Offene Informationsgesellschaft und Terrorbekämpfung – ein Widerspruch?*, MARITIM Hotel Bellevue, Kiel: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2007, URL: https://www.datenschutzzentrum.de/sommerakademie/2007/sak2007-hansen-krause-online-durchsuchung.pdf.

Hansen, Markus und Andreas **Pfitzmann**: „Techniken der Online-Durchsuchung", in: *Online Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008*, hrsg. von Fredrik **Roggan**, Berliner Wissenschafts-Verlag, 2008.

Hedtstück, Ulrich: *Einführung in die theoretische Informatik, Formale Sprachen und Automatentheorie*, Oldenbourg: Wissenschaftsverlag, 2007.

Klimant, Herbert, Rudi **Piotraschke** und Dagmar **Schönfeld**: *Informations- und Kodierungstheorie*, 3. Aufl., Wiesbaden: Teubner, 2006.

Klumpp, Dieter, Hrsg.: *Informationelles Vertrauen in der Informationsgesellschaft*, Springer, 2008.

Kuhlen, Rainer: *Die Konsequenzen von Informationsassistenten*, Suhrkamp Verlag, 1999.

Kurz, Constanze: „Die Geister die ich rief... Deine Spuren im Netz, Symposium 2007", in: *Persönlichkeit im Netz, Sicherheit – Kontrolle – Transparenz*, Düsseldorf: Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, 2008.

Kurz, Constanze: *Kernbereichsschutz, Vortrag auf der „Neue Richtervereinigung"-Mitgliederversammlung im März 2009*, transcript-verlag, März 2009.

Meyer-Schönberger, Victor: *Nützliches Vergessen, Keynote auf der Re:publika 08*, Berlin, 2008.

Mill, John Stuart: *Über die Freiheit*, Reclam Verlag, 1986.

Mxatone und **IvanLeFou**: „Stealth Hooking: another way to subvert the Windows kernel", in: *Phrack Magazine* 0x0c.0x41 (65) (), Phile 0x04 of 0x0f.

Pfitzmann, Andreas: *Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft*, 1. Aufl., Dresden: Lehrstuhl Datenschutz und Datensicherheit, 26.9.2007.

Pfitzmann, Andreas: *Rede vor dem Bundesverfassungsgericht als Sachverständiger zur Online-Durchsuchung*, Karlsruhe, 10.10.2007.

Pfitzmann, Andreas: *Skript zu den Vorlesungen Datensicherheit und Kryptographie*, Karlsruhe, Hildesheim, Dresden, 1990-2000, URL: `http://dud.inf.tu-dresden.de/~pfitza/DSuKrypt.pdf`.

Pieroth, Bodo und Bernhard **Schlink**: *Grundrechte, Staatsrecht II*, 26. Aufl., Heidelberg: C.F. Müller, 2010.

Pohl: „Zur Technik der heimlichen Online-Durchsuchung", in: *DuD — Datenschutz und Datensicherheit* 9.31 (2007), S. 684–688.

Roggan, Fredrik: „Legalisierung im Polizei- und Geheimdienstrecht", in: *Online Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008*, hrsg. von Fredrik **Roggan**, Berlin: Berliner Wissenschafts-Verlag, 2008.

Schaar, Peter: *Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Gesetzentwurf der Fraktionen der CDU/CSU und der SPD: Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, BT-Drs. 16/9588*, Berlin, 15.9.2008.

Schneier, Bruce: *Secrets and Lies, Digital security in a networked world*, Indianapolis: Wiley, 2004.

Sieber, Ulrich: *Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen*, Freiburg im Breisgau, 9.10.2007.

Silberschatz, Abraham, Peter B. **Galvin** und Greg **Gagneand**: *Operating System Concepts*, 8. Aufl., Wiley, 2009.

Bayerisches Staatsministerium der Justiz und für Verbraucherschutz: *Drucksache 16/8125, Antwort des Staatsministeriums der Justiz und für Verbraucherschutz auf die Schriftliche Anfrage der Abgeordneten Susanna Tausendfreund BÜNDNIS 90/DIE GRÜNEN vom 17.02.2011*, Bayerischer Landtag, 16. Wahlperiode, 29.04.2011.

Stark, Holger: „Digitale Spionage", in: *Der Spiegel* 11 (2009), S. 32–34.

Strafrechtsausschuss der Bundesrechtsanwaltskammer: *Stellungnahme der Bundesrechtsanwaltskammer zur sogenannten Online-Durchsuchung*, BRAK-Stellungnahme-Nr. 4/2007, März 2007.

Strafrechtsausschuss der Bundesrechtsanwaltskammer: *Stellungnahme der Bundesrechtsanwaltskammer zur sogenannten Online-Durchsuchung durch das Bundeskriminalamt zwecks Abwehr von Gefahren des internationalen Terrorismus*, BRAK-Stellungnahme-Nr. 42/2007, Oktober 2007.

Tanenbaum, Andrew S.: *Modern operating systems*, 3. Aufl., Pearson Prentice-Hall, 2008.

Thompson, Ken: „Reflections on Trusting Trust“, in: *Communication of the ACM* 27.8 (Aug. 1984), S. 761–763.

Wiegerling, Klaus u. a.: „Ubiquitärer Computer – Singulärer Mensch“, in: *Informationelles Vertrauen in der Informationsgesellschaft*, hrsg. von Dieter **Klumpp**, Springer, 2008, S. 71–84.

Krasemann, Henry und Jörg **Ziercke**: *Interview u. a. zur Online-Durchsuchung*, MARITIM Hotel Bellevue, Kiel: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2007, URL: https://www.datenschutzzentrum.de/sommerakademie/2007/video/sak2007-interview-ziercke.html.

Ziercke, Jörg: *Sprechzettel für die Teilnahme des Präsidenten des Bundeskriminalamtes Jörg Ziercke an der 53. Sitzung des Innenausschusses zu TOP 24a (24b, 24c)*, Berlin, 19.10.2011.

Urteile

Bundesgerichtshof: *Kein heimlicher Zugriff auf ein Computersystem zum Zwecke der Strafverfolgung, 1 BGs 184/06*, HRR-Strafrecht.de, 25.11.2006, URL: http://www.hrr-strafrecht.de/hrr/1/06/1-bgs-184-2006.php.

Bundesverfassungsgericht: *Bundesverfassungsgerichtsurteil zu Verbindungsdaten, BVerfG, 2 BvR 2099/04*, 2.3.2006, URL: http://www.bundesverfassungsgericht.de/entscheidungen/rs20060302_2bvr209904.html.

Bundesverfassungsgericht: *Bundesverfassungsgerichtsurteil zum Beischlaf zwischen Geschwistern, 2 BvR 392/07*, 26.2.2008, URL: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080226_2bvr039207.html.

Bundesverfassungsgericht: *Bundesverfassungsgerichtsurteil zum großen Lauschangriff, BVerfG, 1 BvR 2378/98*, 3.3.2004, URL: http://www.bundesverfassungsgericht.de/entscheidungen/rs20040303_1bvr237898.html.

Bundesverfassungsgericht: *Bundesverfassungsgerichtsurteil zum Mithören an Telekommunikationseinrichtungen, BVerfG 1 BvR 1611/96 u. 1 BvR 805/98*, 9.10.2002, URL: http://www.bundesverfassungsgericht.de/entscheidungen/rs20021009_1bvr161196.html.

Bundesverfassungsgericht: *Bundesverfassungsgerichtsurteil zum Tagebuchinhalt I, 2 BvR 1062/87*, BVerfGE 80, 367, 14.9.1989, URL: http://www.servat.unibe.ch/dfr/bv080367.html.

Bundesverfassungsgericht: *Bundesverfassungsgerichtsurteil zum Tagebuchinhalt II, 2 BvR 147/06*, 1.2.2006, URL: http://www.bundesverfassungsgericht.de/entscheidungen/rk20060201_2bvr014706.html.

Bundesverfassungsgericht: *Bundesverfassungsgerichtsurteil zur Durchsuchung, BVerfG 2 BvR 1011/10*, 5.5.2011, URL: http://www.bundesverfassungsgericht.de/entscheidungen/rk20110505_2bvr101110.html.

Bundesverfassungsgericht: *Bundesverfassungsgerichtsurteil zur Online-Durchsuchung, BVerfG, 1 BvR 370/07*, 27.2.2008, URL: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

Bundesverfassungsgericht: *Bundesverfassungsgerichtsurteil zur Volkszählung, 1 BvR 209, 269, 362, 420, 440, 484/83*, BVerfGE 65, 1, 15.12.1983, URL: http://www.servat.unibe.ch/dfr/bv065001.html.

Onlinequellen

46halbe: *Chaos Computer Club: HSG Wahlsysteme bestätigt Unzulänglichkeit ihrer Wahlcomputer, ccc.de*, 16.10.2006, URL: http://ccc.de/updates/2006/wahlcomputer2 (besucht am 11. 11. 2011).

afp (Agence France-Presse): *Baden-Württemberg stoppt den Trojaner-Einsatz, Badische-zeitung.de*, 10.10.2011, URL: http://www.badische-zeitung.de/nachrichten/deutschland/baden-wuerttemberg-stoppt-den-trojaner-einsatz--50456952.html (besucht am 11. 11. 2011).

ap (The Associated Press): *Viruses Frame PC Owners for Child Porn, Cbsnews.com*, 9.11.2009, URL: http://www.cbsnews.com/stories/2009/11/09/tech/main5589403.shtml?tag=cbsnewsLeadStoriesAreaMain;cbsnewsLeadStoriesHeadlines (besucht am 11. 11. 2011).

Apple Inc.: *Learn more about Siri, Siri is the intelligent personal assistant that helps you get things done just by asking*, 2011, URL: http://www.apple.com/iphone/features/siri-faq.html (besucht am 8. 11. 2011).

Bachfeld, Daniel: *Verräterische Metadaten aus Web-Dokumenten extrahieren, Heise.de*, 26.4.2011, URL: http://www.heise.de/security/artikel/Verraeterische-Metadaten-in-Unternehmensdokumenten-1229482.html (besucht am 8. 11. 2011).

Bernauer, Alexander und Ansgar **Wiechers**: *Personal Firewalls versagen*, 13.12.2004, URL: http://ulm.ccc.de/ChaosSeminar/2004/12_Personal_Firewalls (besucht am 8. 11. 2011).

Blenkers, Eduard: *Tatort Internet, S02E02: Ferngesteuert*, 22.8.2011, URL: http://www.heise.de/security/artikel/Tatort-Internet-Ferngesteuert-1320475.html (besucht am 8. 11. 2011).

Borchers, Detlef und Jo **Bager**: *Bürgerrechtler diskutieren mit BKA-Chef über Online-Durchsuchung, Heise.de*, 22.9.2007, URL: http://www.heise.de/newsticker/meldung/Buergerrechtler-diskutieren-mit-BKA-Chef-ueber-Online-Durchsuchung-177989.html (besucht am 8. 11. 2011).

Borchers, Detlef und Jürgen **Kuri**: *Generalbundesanwältin fordert Vertrauen in Ermittlungsmaßnahmen, Heise.de*, 3.10.2008, URL: http://www.heise.de/newsticker/meldung/Generalbundesanwaeltin-fordert-Vertrauen-in-Ermittlungsmassna 214473.html (besucht am 8. 11. 2011).

Borchers, Detlef und Jürgen **Kuri**: *Kriminalbeamte fordern Verstärkung am digitalen Tatort, Heise.de*, 27.10.2011, URL: http://www.heise.de/newsticker/meldung/Kriminalbeamte-fordern-Verstaerkung-am-digitalen-Tatort-1367798.html (besucht am 8. 11. 2011).

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.: *39 Prozent der Personalchefs verlangen Bewerbung per Internet*, 2.5.2011, URL: http://www.bitkom.org/67820_67810.aspx (besucht am 11. 11. 2011).

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.: *Halb Deutschland ist Mitglied in sozialen Netzwerken*, 13.4.2011, URL: http://www.bitkom.org/de/presse/8477_67667.aspx (besucht am 11. 11. 2011).

Chaos Computer Club: *Chaos Computer Club analysiert Staatstrojaner, ccc.de*, 8.10.2011, URL: http://www.ccc.de/de/updates/2011/staatstrojaner (besucht am 8. 11. 2011).

cristop5: *IPCC's Ben Santer admits GW hoax, Youtube.com*, 17.8.2011, URL: http://www.youtube.com/watch?v=Pj8GlqiOAIs (besucht am 11. 11. 2011).

dapd/dpa: *Minister mokiert sich über Chaos Computer Club, Spiegel.de*, 16.10.2011, URL: http://www.spiegel.de/netzwelt/netzpolitik/0,1518,792072,00.html (besucht am 8. 11. 2011).

Das Bundesamt für Sicherheit in der Informationstechnik: *Aufgaben des BSI, Bsi.bund.de*, 2011, URL: https://www.bsi.bund.de/DE/DasBSI/Aufgaben/aufgaben_node.html (besucht am 8. 11. 2011).

dpa (Deutsche Presse Agentur): *Geheimdienste spitzeln schon seit Jahren, Stern.de*, 25.4.2007, URL: http://www.stern.de/digital/online/online-durchsuchungen-geheimdienste-spitzeln-schon-seit-jahren-587865.html (besucht am 8. 11. 2011).

Eikenberg, Ronald: *Die Rückkehr des BIOS-Trojaners, Heise.de*, 12.9.2011, URL: http://www.heise.de/newsticker/meldung/Die-Rueckkehr-des-BIOS-Trojaners-1341262.html (besucht am 8. 11. 2011).

Eikenberg, Ronald: *Microsoft-Bericht: Fast die Hälfte der Anwender infiziert ihre Rechner selbst, Heise.de*, 13.10.2011, URL: http://www.heise.de/security/meldung/Microsoft-Bericht-Fast-die-Haelfte-der-Anwender-infiziert-ihre-Rechner-selbst-1360040.html (besucht am 8. 11. 2011).

Exif.org: *Exif Specifications, Exif.org*, 2003, URL: http://www.exif.org/specifications.html (besucht am 8. 11. 2011).

Grell, Detlef: *Harsche Kritik an Online-Durchsuchungen, Heise.de*, 3.2.2007, URL: http://www.heise.de/newsticker/meldung/Harsche-Kritik-an-Online-Durchsuchungen-142144.html (besucht am 11. 11. 2011).

Heinrich, Claus: *Chaos Computer Club knackt Bundestrojaner, Tagesschau.de (SWR)*, 9.10.2011, URL: http://www.tagesschau.de/inland/trojaner100.html (besucht am 10. 11. 2011).

Hessischer Rundfunk & ZDF: *ARD/ZDF-Onlinestudie 2011, Fernsehinhalte im Internet in Deutschland immer beliebter*, 2011, URL: http://www.ard-zdf-onlinestudie.de/index.php?id=326 (besucht am 8. 11. 2011).

Hoffmann, Christiane und Stefan **Tomik**: *„Es gibt keine rechtliche Grauzone“, Faz.net*, 15.10.2011, URL: http://www.faz.net/aktuell/politik/im-interview-bundesinnenminister-friedrich-csu-es-gibt-keine-rechtliche-grauzone-11494291.html (besucht am 8. 11. 2011).

Huber, Mathias: *GNOME Zeitgeist – Eine neue Art des Findens, Linux-magazin.de*, 5.7.2009, URL: http://www.linux-magazin.de/NEWS/Desktop-Summit-Gnome-Zeitgeist-schaut-dem-User-auf-die-Finger (besucht am 8. 11. 2011).

Kaiser, Michael: *Small and Midsized Businesses Aware of Security Risks, But Not Doing All They Can to Protect Information, Staysafeonline.org*, URL: http://www.staysafeonline.org/blog/small-and-medium-size-businesses-are-vulnerable (besucht am 11. 11. 2011).

Kleinz, Torsten und Michael **Wilde**: *Virenmail mit Verweis auf Bundestrojaner, Heise.de*, 5.5.2007, URL: http://www.heise.de/security/meldung/Virenmail-mit-Verweis-auf-Bundestrojaner-175374.html (besucht am 8. 11. 2011).

Krempl, Stefan: *Britische Regierung drängt auf EU-weite heimliche Online-Durchsuchungen, Heise.de*, 5.1.2009, URL: http://www.heise.de/security/meldung/Britische-Regierung-draengt-auf-EU-weite-heimliche-Online-Durchsuchungen-193516.html (besucht am 8. 11. 2011).

Krempl, Stefan: *Medienbericht: BND hat bereits Online-Razzien durchgeführt, Heise.de*, 5.1.2008, URL: http://www.heise.de/newsticker/meldung/Medienbericht-

BND-hat-bereits-Online-Razzien-durchgefuehrt-175499.html (besucht am 8. 11. 2011).

Krempl, Stefan und Peter-Michael **Ziegler**: *Bayerischer Landtag setzt den "Bayerntrojaner"frei, Heise.de*, 3.7.2008, URL: http://www.heise.de/newsticker/meldung/Bayerischer-Landtag-setzt-den-Bayerntrojaner-frei-183633.html (besucht am 8. 11. 2011).

Krempl, Stefan und Peter-Michael **Ziegler**: *Bundesrat will heimliche Online-Durchsuchungen auf Terrorabwehr beschränken, Heise.de*, 4.7.2008, URL: http://www.heise.de/newsticker/meldung/Bundesrat-will-heimliche-Online-Durchsuchungen-auf-Terrorabwehr-beschraenken-183867.html (besucht am 11. 11. 2011).

Krempl, Stefan und Peter-Michael **Ziegler**: *Noch viele Fragen offen bei heimlichen Online-Durchsuchungen, Heise.de*, 15.9.2008, URL: http://www.heise.de/security/meldung/Noch-viele-Fragen-offen-bei-heimlichen-Online-Durchsuchungen-205825.html (besucht am 8. 11. 2011).

Kruse, Peter: *This is how Windows get infected with malware, CSIS Security Group*, 27.9.2011, URL: http://www.csis.dk/en/csis/news/3321 (besucht am 8. 11. 2011).

Köhntopp, Kristian und Marit **Köhntopp**: *Why Internet Content Rating and Selection does not work, Koehntopp.de*, 1999, URL: http://kris.koehntopp.de/artikel/rating_does_not_work/ (besucht am 8. 11. 2011).

Mühlbauer, Peter: *Wo und wie der Bayerntrojaner zum Einsatz kommt, Telepolis/Heise.de*, 3.3.2011, URL: http://www.heise.de/tp/artikel/34/34289/1.html (besucht am 8. 11. 2011).

O. V.: *Verschwundene Festplatte offenbar noch in Kopie vorhanden, Spiegel.de*, 26.4.2000, URL: http://www.spiegel.de/politik/deutschland/0,1518,74256,00.html (besucht am 11. 11. 2011).

Patalong, Frank: *Behörden spähten 100-mal Computer aus, Spiegel.de*, URL: http://www.spiegel.de/netzwelt/netzpolitik/0,1518,791941,00.html (besucht am 8. 11. 2011).

Poulsen, Kevin: *Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years, Wired.com*, 16.4.2009, URL: http://www.wired.com/threatlevel/2009/04/fbi-spyware-pro (besucht am 8. 11. 2011).

Rath, Christian: *"Terroristen sind auch klug", Taz.de*, 8.2.2007, URL: http://www.taz.de/1/archiv/archiv/?dig=2007/02/08/a0169 (besucht am 8. 11. 2011).

Rath, Christian: *„Am Computer des Täters ansetzen“, TAZ.de*, 26.3.2007, URL: http://www.taz.de/1/archiv/?id=archivseite&dig=2007/03/26/a0119 (besucht am 8. 11. 2011).

Ries, Uli und Daniel **Backfeld**: *Bootkit hebelt Festplattenverschlüsselung aus, Heise.de*, 30.7.2009, URL: http://www.heise.de/security/meldung/Bootkit-hebelt-Festplattenverschluesselung-aus-748859.html (besucht am 8. 11. 2011).

Rötzer, Florian: *Innenministerium: Verfassungsschutz, MAD und BND können Online-Durchsuchungen durchführen, Heise.de*, 24.3.2007, URL: http://www.heise.de/newsticker/meldung/Innenministerium-Verfassungsschutz-MAD-und-BND-koennen-Online-Durchsuchungen-durchfuehren-161153.html (besucht am 8. 11. 2011).

Schmidt, Jürgen: *Microsoft bestätigt USB-Trojaner-Lücke, Heise.de*, 17.7.2010, URL: http://www.heise.de/security/meldung/Microsoft-bestaetigt-USB-Trojaner-Luecke-1039915.html (besucht am 8. 11. 2011).

Schulzki-Haddouti, Christiane und Peter-Michael **Ziegler**: *Bundesinnenminister warnt vor zunehmender Netzspionage, Heise.de*, 22.5.2007, URL: http://www.heise.de/security/meldung/Bundesinnenminister-warnt-vor-zunehmender-Netzspionage-131409.html (besucht am 23. 11. 2011).

Stegers, Fiete: *Das iPhone als Spitzel, tagesschau.de*, 21.4.2011, URL: http://www.tagesschau.de/inland/iphone116.html (besucht am 8. 11. 2011).

Wegener, Christoph: *Vortrag: Hackerparagraph und Online-Durchsuchung, Rechtsunsicherheit in der IT-Branche*, 8.5.2008, URL: http://www.guug.de/lokal/hamburg/talks/SGLH2008-HuO.pdf (besucht am 8. 11. 2011).

Werner, Tillmann: *Federal Trojan's got a "Big Brother", Securelist.com*, 18.10.2011, URL: http://www.securelist.com/en/blog/208193167/Federal_Trojan_s_got_a_Big_Brother (besucht am 8. 11. 2011).

Wilkens, Andreas: *Mehr als 50 Millionen Internetnutzer in Deutschland*, 4.7.2011, URL: http://www.heise.de/newsticker/meldung/Mehr-als-50-Millionen-Internetnutzer-in-Deutschland-1273106.html (besucht am 8. 11. 2011).

Wilkens, Andreas: *Verfassungsschutz klärt über Wirtschaftsspionage und Such-Trojaner auf, Heise.de*, 16.3.2007, URL: http://www.heise.de/newsticker/meldung/Verfassungsschutz-klaert-ueber-Wirtschaftsspionage-und-Such-Trojaner-auf-157823.html (besucht am 8. 11. 2011).

ZDF: *Politbarometer 14.10.201, zdf.de*, 14.10.2011, URL: http://wahltool.zdf.de/Politbarometer/mediathekflash.shtml?2011_10_14 (besucht am 8. 11. 2011).

Sonstiges

Beyer, Michael und Kay **Walter**: *Videobeitrag: Wanze im Wohnzimmer – Online-Spitzelei durch den Verfassungsschutz, RBB Kontraste, Beitrag 02*, 10.5.2007.

Kurz, Constanze und Ulf **Buermeyer**: *Vortrag: Das Grundrecht auf digitale Intimsphäre, Festplattenbeschlagnahme in neuem Licht*, 27.12.2008, URL: `http://events.ccc.de/congress/2008/Fahrplan/events/2923.en.html`.

Sentker (Die ZEIT), Andreas und Ulrich (Deutschlandfunk) **Blumenthal**: *Diskussion: Vertraue niemandem – Mit Sicherheit im Netz, 32. ZEIT-Forum der Wissenschaft*, 12.12.2008.

Abbildungsverzeichnis

Tabellenverzeichnis

Vielen Dank an ennA, HK, loco, crk, muva, 46halbe, sak, mnass, das Läubchen und vor allem W.